

Dickson, 'Police access to NHS confidential medical records – a question of public interest.' [2010] 4 *Web JCLI*  
<http://webjcli.ncl.ac.uk/2010/issue4/dickson4.html>

## Police access to NHS confidential medical records – a question of public interest.

Lisa Dickson

Lecturer in Law  
Kent Law School,  
University of Kent

L.M.Dickson@kent.ac.uk

Copyright © 2010 Lisa Dickson

First published in Web Journal of Current Legal Issues

---

### Summary

This article considers the oversight and monitoring of police requests as second users for identifiable personal information held by any arm of the NHS. Though there has been much recent interest in the related area of the police collation, retention and use of the DNA database, there has been comparatively little attention given to police access to data sets in which they are not first user, of which NHS records are a principal example. The paper draws attention to the fragmented manner in which central oversight and monitoring is pursued by the NHS in relation to police requests. Thus, with regard to requests falling within the ambit of s.251 of the NHS Act 2006, central monitoring is ensured under the Terms of Reference of the Ethics and Confidentiality Committee of the NHS. In contrast, for requests that are made other than for medical purposes no such system is in place. It is suggested that this absence is a serious omission, with implications both for NHS officers charged with handling such requests as they are unable to draw upon comparisons in deliberating disclosure, and for the public in the confidence they should have in robust protection of patient confidentiality.

---

## Contents

Introduction

NHS Act 2006 s.251 - use of data for medical research

Police access to Oyster card information.

Police Requests for Disclosure

Conclusions

Bibliography

---

## Introduction

In recent years there has been much debate on the issue of access to confidential information held by the state on individual citizens (see for example, Second Report 2009, Anderson et al 2009, Booth 2003). Media attention has highlighted concerns ranging from the very general, e.g. the security of the information held, to the specific, e.g. whose information should be retained on the National DNA Database, and in what circumstances is its release warranted (see Annas 2009, Hepple 2009). Some scrutiny has focused on medical records held by the NHS, and the security of the National IT NHS programme has garnered criticism from many quarters with concern focussing on the inadvertent loss of data or the way in which staff within the NHS share data (see ICO press release 15 June 2010, ICO Press release 15 July 2009, Wheeler 2008). However, much less consideration has been given to the intentional release by the NHS of patient-identifiable information to third parties (i.e. second users). Such release includes the sensitive case of release to the police of confidential patient records without the consent of the patient. In light of widespread concern over privacy issues and control of confidential information, the present article examines NHS rules and procedures controlling police access in these cases.

NHS control of access to its records is only partial, as in their pursuit of crime police may seek a court order for the release of confidential medical information that is germane to their enquiry (s.9 and Schedule 1 of PACE 1984). (For the purposes of this article the notion of medical records is taken to include sensitive patient-identifiable information which can be held on any of the NHS databases or indeed the more traditional patient medical records. This includes, for example, Detailed Care Records, Summary Care Records and any other information contained on the NHS 'Spine'. The NHS is currently undergoing a move to medical records to an electronic format and information is recorded in a number of different ways.) This route to accessing confidential medical information ensures that the decision as to whether release is necessary is made within the arena of the court, thus removing the decision from NHS staff – a warrant issued pursuant to section 9 compels the disclosure of the information

in question. However, if the police do not present a warrant compelling the disclosure of identifiable patient information they are entitled to *request* that the information is disclosed to them under the provisions of s.29(3) of the Data Protection Act 1998. Though a health care professional is under no obligation to release the requested information to the police under the provisions of s.29, they may do so where the patient concerned has given consent, or where the patient's interest in non-disclosure and/or the public's interest in maintaining patient confidentiality is outweighed by some other greater public interest. In the present example the competing public interest would be that of the detection of serious crime. It is, then, with these public interest requests that this article is primarily concerned.

As little attention has so far been paid to police requests to the NHS for access to confidential records, it will be useful to set out detail of the procedures followed by the NHS and its officers in determining whether to grant access in these cases. These procedures are set out in section 3. However, the article also aims to show that the procedures governing these cases are inconsistent with procedures in place to govern access to confidential information in other areas. Hence the paper opens in section 2 with an examination of the processes in place to control access to information in two parallel cases. The first concerns the NHS process that must be engaged in deliberating access by second users to patient-identifiable information for the purposes of medical research. This takes place under the provisions of section 251 of the National Health Services Act 2006. The second case falls outside the NHS, and concerns the procedures in place governing police access to confidential customer information held through London Transport's Oyster Card travel card. As the first deals with access to information solely for the purposes of medical research rather than prevention of crime, and as the second concerns travel information rather than confidential medical information, it might be supposed that procedures and monitoring in these cases would not be more rigorous and transparent than in the case principally in question. This is not so, however, and the most fundamental distinctions between the processes are noted in section 3, where detailed attention is given to the protocols, practices and monitoring arrangements presently in place to regulate the disclosure to police of confidential information without a patient's consent. The paper closes in section 4 by drawing conclusions from the study, locating these in the context of wider concerns about privacy and information access.

## **NHS Act 2006 s.251 - use of data for medical research**

A useful mechanism for considering the shortcomings of the protocols in place for police access is firstly to look at the provisions in place elsewhere in the NHS, in which access may similarly be given to patient-identifiable data without the subject's consent. The obvious area for comparison is therefore requests made by medical researchers for access to patient-identifiable data for purposes other than patient care. Whereas police are permitted to request access to confidential data without patient consent when it is deemed necessary to police investigations of crime, researchers can request access to the same patient information for the purposes of medical research. While much medical research is conducted using anonymous data, for the purposes of some studies person-identifiable indicators are important, for example cancer registers (see the

National Cancer Information Service and Haynes et al 2007) where tracing geographical location and perhaps family connections is imperative to greater understanding of the disease. Where identifiable data is utilised an obvious route for researchers is to seek the consent of the patients or data subjects involved, but in larger or more complex studies, such an undertaking may prove impractical or indeed impossible. The problems associated with obtaining consent from patients for inclusion in such research is well documented (see Baird 2009, Stone 2005, Davies 2006 and Kalra 2006). Researchers seeking to use patient-identifiable data without consent for the purposes of medical research are thus able to request the information courtesy of the Data Protection Act 1998 (see schedule 3 section 8) through a provision that is similar to that of police requests in the investigation of crime. However, at this point the two forms of request diverge.

In the case of medical research requests for access are put on a formal statutory foundation, requiring that release of patient-identifiable data for the purposes of medical research obtain support under s251 of the National Health Services Act 2006. This was previously s60 of Health and Social Care Act 2001, approval being administered by the now defunct Patient Information Advisory Group (PIAG). Although the provisions of the NHS Act only date from 2006 the new legislation mirrors its predecessor and the procedures followed by the NIGB Ethics and Confidentiality Committee are also based on the previous scheme with member of PIAG being invited to join the new ECC at its inception. The new provision permits the Secretary of State to set aside the expected duty of confidentiality for particular classes of information sharing and provides

“a secure legal basis for disclosure of confidential patient information for medical purposes, where it was not possible to use anonymized information and where seeking consent was not practicable” (see NIGB ECC terms).

Although approval is given by the Secretary of State, applications are formally administered by the National Information Governance Board for Health and Social Care (NIGB) who advise the Secretary of State on when support should be given. Section 251 support ensures that the individuals or organisations providing and using the sensitive data are protected by law from legal challenges from an individual patient on the grounds of breach of confidence. This section 251 approval does not mean that the organisation holding the requested data *must* provide the information but it does provide surety for those who provide (and are granted access to) the data that the request has been considered and deemed suitable for protection from claims of breach of confidentiality. This is a level of certainty and protection, as we shall see, that is not afforded to those individuals who consent to police access to the same form of patient-identifiable information for different purposes.

Each section 251 application is considered centrally by NIGB's Ethics and Confidentiality Committee (ECC) ensuring that all applications, no matter where in the country the request comes from, are considered by the same committee with the expertise and experience to consider the request and ensure that the all applications are determined to the same standard. Although NIGB and the ECC only took over responsibility for section 251 requests from the Patient Information Advisory Group (PIAG) in January 2009, the Committee

have a well established applications procedure for section 251 approval based on that developed by PIAG. These procedures require not only a clear explanation by the applicant of the purpose for which the information is required but also require evidence of the parameters of the study and evidence of security protocols being put in place, together with a requirement for annual review of all section 251 approvals to ensure that the identifiable data is still required and that the conditions for initial approval are still being met (see NIGB ECC Applications Information). In short, in order to obtain section 251 protection, successful applicants not only have to provide reasons why the information is necessary but must also account for the precise use to which it will be put, showing evidence of how the continued security of the information will be ensured, with the entire application and this information subject to an annual review. Not only are rigorous procedures and requirements in place for *applicants* seeking patient-identifiable data, but the monitoring of both decisions made and of the continued use of the information is assured through reporting mechanisms such as the NIGB annual report. This form of reporting provides only bald statistics. The ECC reported that in the first ten months of 2009 the Committee administered 72 applications for s251 support, of which 42 were approved, 20 declined with the remaining number either deemed not to require approval or pending further outcome (NIGB Annual Report 2009, p16). However, it does provide an effective overview of the use of the section 251 process and gives a broad sense of whether access is being recommended by the ECC, and in this way presents a form of easily accessible monitoring. National statistical information is available for inspection, as are the minutes to ECC meetings reporting variations to section 251 support and review of individual projects.

Members of the ECC must engage the same question of balance as that required of those determining whether police access to confidential medical information should be permitted. The difficulty in deliberating under section 251 whether the public interest in disclosure overrides that of maintained confidentiality is recognised by NIGB:

“The use of section 251 is an important function and many factors need to be taken into account when considering applications. The skills and experience needed to assess applications take some time to build up.”  
(NIGB Annual Report 2009 p16).

It will be useful to bear in mind these observations when we come to consider the procedures attending police requests for information under the Data Protection Act 1998 in section 3.

### **Police access to Oyster card information.**

Formalised regulation and monitoring of access to information held on individuals is, of course, not only found in the field of sensitive medical information. For example, requests for records of personal information and train journeys made by holders of Transport for London’s ‘Oyster Card’ travel system are also subject to rigorous control, providing illustration of how another database of information processes second use police requests for confidential identifiable information.

Police are able to make use of confidential personal information from the Oyster card system operated by Transport for London (TfL). The Oyster card, introduced in 2003, is a pre-paid ticketing system which allows card holders to travel on all forms of transport within London, including London buses, trams, the Docklands light railway and boats. The Oyster card automatically logs journeys when it is swiped and retains the journey information, linked to a customer account, for a period of 8 weeks (see TfL terms). The benefits such information may provide to police investigations is clear. Thus, for example, city solicitor Tom Rhys-Pryce was murdered at Kensal Green tube station in January 2006. As the 2 individuals responsible for his murder then made use of the victim's Oyster card, police were able to access cctv footage based on the electronic information tracking the use of the Oyster card (see 'Oyster data is 'new police tool'' BBC News 13 March 2006). The increase in recent years of police requests for access to journey log information suggests that the police are making greater use of this information held by Transport for London. In 2006 Transport for London reported that in 2004 only 7 information requests had been made by police this number had increased. More recently numbers of police requests made to TfL have been provided as a generic number of total requests for confidential information, rather than broken down into particular areas such as Oyster card journeys or CCTV information. The total number of requests received by TfL from police forces in 2007 was 5,109 and in 2008 it was 6,311 (see FoI request TfL 90319, response received 19 May 2009). However, the system for permitting police access to the information contained on Oyster cards is markedly different to that used in accessing confidential medical information through NHS personnel without a court order.

Transport for London has a dedicated Data Protection and Disclosures Team who process and determine all requests for confidential information, from police and other organisations. In this way the process for access to the confidential information mirrors that of researchers seeking section 251 assistance as in both cases a dedicated team exists through which all requests are processed. This allows a body of expertise to develop and encourages a consistency of approach. The Transport for London's own terms and conditions explain how requests are processed – “the police have to demonstrate that the personal data concerned will assist them in the prevention or detection of a specific crime, or in the apprehension or prosecution of an offender” (see TfL, Oyster card terms and conditions). Information is also provided as to the approximate numbers of requests granted, with TfL commenting that “we reject about five to ten percent of requests each month because the police do not provide acceptable levels of detail or, we deem the requests excessive” (TfL terms).

While the information required by Transport for London does not differ greatly from that requested by NHS organisations, in that reasons as to why the information is necessary must be provided, there remains one area in which TfL proves more robust. Transport for London has a dedicated and discrete team who determine all the decisions as to whether to disclose, a team which is able to build up a body of decisions as to when to disclose and able to take into account a history of decisions, allowing for a more coherent and consistent approach to balancing competing interests, even on a case by case basis.

## Police Requests for Disclosure

The present article aims principally to elucidate how the NHS processes police requests for access to patient-identifiable information without the consent of the patient. Having briefly considered two comparable cases in section 2, NHS policy and procedure must now be articulated for the cases chiefly in issue. However here we encounter an immediate difficulty, for no single, determinate procedure exists to be elucidated: no centralised process has been mandated under which the relevant requests are to be processed. Instead, police requests to the NHS for disclosure of information are decided on the basis of procedures drafted locally by organisations within the NHS, by staff accepted as suitable by the health body in question, operating under procedures that may have little in common even with those of neighbouring departments or trusts. There is no provision for national comparison of the decisions reached and the manner in which they were achieved, nor is there even a centralised record of these decisions. Frontline staff who are called upon to deliberate a request thereby meet with widely varying levels of documentary advice and assistance, and must operate within structures that show striking variance between organisations. In consequence of the fragmentary and uneven nature of the relevant processes in use throughout the health service, a comprehensive description is impossible within the space here, but some principal features can still be drawn.

The document that directly informs NHS organisations' present practices in these cases is the Department of Health's Code of Practice on Confidentiality 2003. Frontline staff deliberating disclosure can find further assistance in the 'Confidentiality and Disclosure of Health Information Tool Kit' published by the British Medical Association in 2009, and also in the General Medical Council document, 'Confidentiality 2009'. In the GMC document the 'emphasis remains firmly on anonymising or coding data, or getting patient's consent wherever practicable. In addition, doctors are advised to seek the advice of experienced colleagues, Caldicott Guardians, or their professional or regulatory body if in doubt. (*Caldicott Guardian Newsletter*, November, 2009, p.9) However the GMC and BMA documentation provides advice and explanation only. The Code is a best practice guidance document targeted at Caldicott Guardians and data protection officers holding posts within individual NHS departments and trusts. Its intention is "to provide guidance to NHS and NHS related organisations on patient information confidentiality issues", which will thus "help send a consistent message across the Service on confidentiality and issues around the processing of patient information" (NHS 2003 pii). The Code deals with all matters of confidentiality that bear upon the health service, and so only a portion of it provides specific information about police requests for access to confidential information where consent has not been given. With regard to the matters of confidentiality treated throughout the Code it is left to individual organisations to draft and stipulate appropriate procedures for staff, so no national, centralised process is established in the document, and nor is one suggested. Thus the Code envisages divergence between organisations regarding the general protocols on confidentiality that might be in place:

"NHS organisations should have developed, or be in the process of developing, information-sharing protocols that set out the standards and procedures that should apply when disclosing confidential patient

information with other organisations and agencies. Staff must work within these protocols where they exist, and within the spirit of this code of practice where they are absent". (NHS 2003 p20)

Moreover, the protocols in question have a very broad scope. For example, the Code advises that, "For all types of records, staff working in offices where records may be seen must: Shut/lock doors and cabinets as required; Wear building passes/ID if issued; Query the status of strangers" and so on (NHS 2003 fig 5, p6). The part of the Code treating disclosure following a police request for access, where patient consent has not been given, is held in Annex B, entitled "Confidentiality Decisions", specifically at B3; that is, "where the purpose is unrelated to healthcare or another medical purpose" (NHS 2003, p28). B3 contains a flowchart outlining the decision-process that is to be followed by a staff member in deliberating disclosure in these cases. Because it is aimed at frontline staff, the chart is appropriately general (for example, asking whether a patient has been informed of the request, and if so, have they consented, and if so, stipulating that the information should be released). However, the elements of the chart dealing with access to the police without consent merely refer a staff member to the ss.30-33 presented below the chart itself. Section 30 sets out the general issue:

"Under common law, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service".

Section 31 stipulates baldly that records must be kept of the decision, including evidence of the reasoning used, whilst section 32 concerns the information to be given to the patient regarding the matter. Section 33 then provides that,

"Each case must be considered on its merits. Decisions will sometimes be finely balanced and staff may find it difficult to make a judgement. It may be necessary to seek legal or other specialist advice (e.g. from professional, regulatory or indemnifying bodies) or to await or seek a court order. Staff need to know who and where to turn to for advice in such circumstances".

Notably, the identification of the 'staff' in question is left open, leaving this central matter for specification (if at all) by the NHS organisation concerned. Equally, the matter of who to turn to is left to the relevant organisation, and no further information, precedent or example is provided about the deliberative process itself. Moreover, section 31 notes that records ought to be kept because,

"It may be necessary to justify such disclosures to the courts or to regulatory bodies and a clear record of the decision making process and the advice sought is in the interest of both staff and the organisations they work within."

This reminds us that for staff deliberating disclosure in these cases there is no legal protection available as there is for those applications for confidential identifiable information approved under section 251.



In light of the discretion left to organisations within the NHS to stipulate procedures governing disclosure, some attention must be given to the protocols that individual organisations have put in place, at least to illustrate the wide variance noted above. Before this, however, note must be made of the role of Caldicott Guardians, for their role is mandated nationally, and so might be imagined to provide consistency across cases alongside the general provisions of the Code.

The question of disclosing confidential medical records and when it should be done was one of the primary issues addressed in the Caldicott review of patient-identifiable information in 1997 (Department of Health (1997)). A key recommendation of the resulting report was the creation of the Caldicott Guardians, individuals within each primary care trust or NHS department who would have responsibility for fundamental aspects of confidentiality and information governance. Under HSC1999/012, dated 22 January 1999, Chief Executives of NHS organisations were instructed to appoint a Caldicott Guardian by 31 March 1999, and from this point Guardians have been tasked with a ‘key role’ in ensuring that,

“organisations satisfy the highest practical standards for handling patient-identifiable information. Acting as the ‘conscience’ of an organisation, the Guardian should also actively support work to facilitate and enable information sharing, and advise on options for lawful and ethical processing of information as required. Local issues will inevitably arise for Caldicott Guardians to resolve. Many of these will relate to the legal and ethical decisions required to ensure appropriate information sharing. (Caldicott Guardian manual, 2010, para.3.1)”

Paragraph 3.5 of the current CG Manual (March 2010) stipulates that, “Staff should be advised to seek assistance from the Caldicott Guardian where necessary; typical examples of such situations are ...a request from the police for access to patient information”.

There are more than 750 Caldicott Guardians currently in place who are, it would seem, well placed to replicate the role assumed by the Ethics and Confidentiality Committee in s251 applications and the Data Protections and Disclosures Team operated by Transport for London. Thus it would seem reasonable to expect, as the Guardians have been in place since 1999, that a coherent, cohesive and transparent system has been put into place to handle police requests for disclosure in the public interest. None, however, is yet in place, and indeed, while the Caldicott Guardians are referred to in both GMC and BMA advice for members (in which staff are advised to seek assistance from the Guardian where possible) this is not echoed in the NHS Code of Practice on Confidentiality. The Code does not require that the Guardian necessarily be part of a team to process police requests, and though mention is made of the Caldicott Report and its principles for disclosure there is no specific requirement or even suggestion that when faced with a ‘finely balanced’ police request staff should seek assistance from the Guardian. So whilst many departments and trusts do ensure that the Guardian is tasked with the responsibility of determining a police request, this is far from a universal picture. The problem then is that many frontline staff called upon to deliberate requests only have recourse to very general protocols and so when approached

by the police, “operational staff members do not refer such approaches to the Caldicott Guardian, (or on-call manager)” (Caldicott Guardian 2007, p16), even though this possibility is always open. As they are of key importance to frontline staff, these protocols now require some attention.

The variance between organisations can be seen in the published protocols of Hampshire Community Health Care Trust’s document, ‘Disclosure of Information to the Police Procedure’ and Central Lancashire PCT’s document, ‘Data Protection and Confidentiality Procedures and Guidelines for Staff’. At 2.2.6 the Central Lancashire protocol states that, for the cases in question,

“...the decision to release information should be referred to the nominated senior individual. This nominated person shall be specified in the procedures of each Partner Agency and will make a judgement on a case-by-case basis. It may be appropriate for this person to seek additional legal or specialist advice if information is to be disclosed without the individual’s consent. A formal record must be kept by the relevant agency as to the reason why a disclosure of personal information was made. Where public interest is the reason, the grounds for doing so should be documented. Each case should be judged on its merits whether a disclosure without consent is justified. Decisions must be made by those with delegated powers within the Trust such as the Caldicott Guardian.”

In contrast, the Hampshire document states at 2.1 that “the Information Governance Manager must be informed of all information requests by the police to any personal or sensitive record or data. This is a statutory requirement under the ‘NHS Code of Confidentiality’”, and continues at 2.4: “Information will not be released unless: the authority of the consultant or senior clinician in charge of the Minor Injuries Unit is obtained”. At 2.6 authorising staff must copy their consent to the request to the Information Governance Manager. So where Central Lancashire PCT demands at least that the relevant decision is taken by “a nominated senior individual” ... “*such as* the Caldicott Guardian” (my italics), Hampshire CHC requires only that the relevant Information Governance Manager is later *informed* about the request and decision which is instead taken by identified frontline medical staff. Hampshire’s document clearly states at 2.2 that “if in doubt staff should seek advice from the Information Governance Manager or On-call Duty Manager”, but there is no mention of the Caldicott Guardian in the process. It is important to note that there is no suggestion here that Hampshire CHC is remiss in its procedures, or indeed that Central Lancashire PCT is remiss either; the point is precisely that both sets of protocols, though showing wide variance in who is tasked to make the relevant decision (including the remit of the Caldicott Guardian), both fit within the very broad scope of the national Code.

The discrepancies noted above carry practical significance, too. For example, the provision in some protocols, stipulating that staff should seek appropriate advice “if in doubt” (e.g. Hampshire CHC at 2.2), requires the staff concerned to have a confident grasp of where requests actually *are* ‘finely balanced’ in order to ensure “that the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential

service” (NHS Code, para 30). Plainly, the opportunity for frontline medical staff to accumulate the experience required for such judgement is, at the very least, short of that likely to be possessed by a Caldicott Guardian, for of course, in some cases it is only experience that might indicate where a police request should be treated as problematic. The variance in protocol is underlined in a final illustration, Humber Mental Health Trust noting in its document ‘Disclosing Information to the Police: Operational Procedure’ at 3.3, that in the cases in question:

“Information should only be supplied to the police if it is in the public interest to do so. The decision should be made by [the] health professional who is responsible for the relevant aspect of the patient’s health care at the time. Further advice may be sought if necessary e.g. Legal Services Manager, Caldicott and Data Protection Officer or Caldicott Guardian. The Caldicott Guardian will make the final decision in complex cases.”

In short, there is a composite and uneven treatment given to police requests in existing protocols under the national NHS Code, with health professionals determining the matter in some cases and nominated officers in others, and with little unanimity on display concerning the role of Caldicott Guardians, even though the Guardians might otherwise help to ensure consistency and build experience across organisations. These matters are of obvious relevance to individuals concerned about the confidentiality of their patient records, but they are also of relevance to the public’s interest in maintaining a confidential health service and to the NHS staff members called upon to deliberate the requests - for it is important to remember that, under the NHS Code, staff adjudicating police access do not have the legal protection that follows the national s.251 procedure for disclosure further to medical research. Even amongst Caldicott Guardians themselves, concern is regularly expressed through their forum of Caldicott Newsletters about how best to balance the competing interests in question whilst ensuring consistency across cases, whilst an Information Governance Manager writing in the Newsletter recently noted that “knowledge around information governance is still, worryingly, very limited and support from the Board and senior managers is in many cases scarce” (Caldicott Guardian, July 2009, p.5). Moreover, the lack of a mandated, national protocol fails to be mitigated by a robust national system of records and reports under which consistency and best practice might be reviewed.

In short, there is no national or centralised monitoring of how decisions are taken, who is taking the decisions, how many decisions are made in favour of disclosure or against, nor of how many requests are received from the police to begin with. There is no process to allow one NHS organisation to seek information from others, and the Caldicott Guardians have no national monitoring remit even for the decisions over which they have scrutiny. Thus the parochial nature of the protocols in place to guide decisions is reflected in the monitoring and reporting arrangements that are or might be in place, though the local nature of the former would seem to press the case for a centralised standing for the latter. Freedom of Information requests made to both the NHS Information Centre and the Department of Health confirmed that “there is no central collating of information carried out ... of police requests to NHS bodies” (NHS – FoI 2010). More concerning is the explanation that “(e)ach individual

PCT or NHS department will have its own IG Directorate therefore, each will have its own mechanisms for recording the types of requests received by police” (NHS – FoI request 2010). So, there is no national recording and reporting mechanism in place which would allow a comparison of requests and percentages granted and indeed no ability to determine whether there is a coherent national approach to the way in which the balance in question is deliberated or monitored in this type of request.

Moreover, freedom of information requests to police forces on the relevant matter elicited a similar response. After contacting their ‘Major Crime Department, Public Protection Unit, and Specialist Operations Department. Kent Police confirmed that the information was not recorded. (Freedom of Information request Kent Police reference 1370/2010 response of 23 March 2010). The Association of Chief Police Officers have also confirmed that they do not hold any information on police forces requests for access to confidential medical information without patient consent. ACPO, as a private company, is not subject to the Freedom of Information Act 2000. However, they were prepared to answer emailed questions (Email response received 23 April 2010). In turning down a similar request to that made of the Kent police on the grounds of cost, the Metropolitan Police noted that “currently this information is not held centrally and to collate it for the purposes of this request would involve a disproportionate effort”, requiring “an individual manual search of every crime file held by the MPS” (MPS FoI 2010). Though this response confirmed those received elsewhere, the MPS statement added that,

“the Metropolitan Police Service is rolling out a programme of standardising the management of police information across the police service, including sharing information with partner agencies. The programme will include a requirement to record requests for/disclosure of police information and to record police requests to other agencies for their information and the responses received. In the case of police requests for other agency information, the record will be held in the most appropriate place but it is not currently planned to hold these centrally” (MPS FoI 2010).

This policy initiative, whilst encouraging, serves also to highlight the piecemeal and uneven nature of existing arrangements across the country, with the concerns that this naturally presents regarding the transparency, accountability and monitoring of data protection issues regarding the release to police of confidential information.

## Conclusions

Following inadvertent and well-publicised data losses, there has been much recent public concern about the protection of confidential information within the NHS. Similar public and media concern has attached to the police’s development and use of DNA and other information databases. However, little attention has so far been paid to the protocols and practices governing the disclosure of information between these two bodies, where the police request disclosure of confidential patient-identifiable information without the consent of the patient concerned. The present paper aims to elucidate these procedures in as much as their general features can be traced in outline, though unifying detail

is difficult because of the localised nature of the processes in place. Of course, the detail of local arrangements within discrete NHS organisations can be accounted for by the very different sizes and remits of the organisations concerned, in which some are national (NHS Direct) and others small, specialized and very local. However, this scope does not account for the differences in approach of similar-sized NHS organisations, even though enquiry shows that neighbouring PCTs have drafted quite different protocols to govern the matter. This inconsistency, together with the hazy mandate given to Caldicott Guardians and the absence of any national monitoring process, appears to be flatly inconsistent with the approach in comparable cases where data protection and confidentiality are issues.

Transport for London has a standing team who determine all the decisions as to whether to disclose information to police without consent. This team is thereby able to build up a body of decisions as to when to disclose, and is able to take into account a history of decisions, allowing for a more coherent and consistent approach to balancing competing interests, whilst fostering conditions for transparency and accountability. Thus TfL is able to provide an approximate number of requests which have been refused, and some indication of a generalised pattern of reasons why the requests were not accommodated. There is recognition of the need for transparency and monitoring in the ability of the organisation to provide an account of police requests for access to confidential information. This recognition is not replicated in the case of police requests for confidential information made to the NHS, though the principles of consistency and accountability, together with the practical advantage of experience, are in evidence in the central, statutory footing for requests made to the NHS under section 251 for the purpose of medical research. At the very least this demonstrates an inconsistency that needs to be justified, for presumably the good reasons for the formal, central procedure in the case of section 251 applications hold as good reasons for a similar procedure where other requests for confidential information are made, particularly if these come from the police. If not, some special argument needs to be raised to account for and defend the distinction; that no argument or defence has presently been made is, perhaps, due to the question never having been put. At any rate, even a circumspect conclusion must note that the existing arrangements fall short of the consistency listed as principal ambition in the NHS Code of 2003 (preamble/Reader Information), and it is, of course, possible to go much further. For not only do present procedures fail to display the robustness needed where privacy and confidentiality are in issue, but they also fail to provide frontline staff with the guidance and support that they require in acquitting their responsibilities. It is little wonder then that a recent GMC poll of GP's discovered that 'knowing when it is in the public interest to breach patient confidentiality' was the topic that most worried GP's during their careers (Durham 2010)

## Bibliography

Anderson, R, Brown, I, Dowty, T, Inglesant, P, Heath, W and Sasse, A (2009) *Database State* – (York: Joseph Rowntree Foundation)

Annas, G. (2009) 'Protecting Privacy and the Public — Limits on Police Use of Bioidentifiers in Europe.' 361(2) *New England Journal of Medicine* 196

- Baird, W, Jackson, R, Ford, H, Evangelou, N, Busby, M, Bull, P and Zajicek, J (2009) 'Holding personal information in a disease-specific register: the perspectives of people with multiple sclerosis and professionals on consent and access' 35 *Journal of Medical Ethics* 92
- Barrett, G, Cassell, J, Peacock, J and Coleman, M (2006) 'National survey of British public's views on use of identifiable medical data by the National Cancer Registry' 332 *British Medical Journal* 1068
- BMA Ethics (2008) *Access to Health Records: Guidance for health professionals in the United Kingdom* (BMA)
- BMA Medical Ethics Committee (2005) *Confidentiality as part of a bigger picture- a discussion paper from the BMA*  
<http://www.bma.org.uk/ethics/confidentiality/ConfidentialityBiggerPicture.jsp>  
(accessed 1 July 2010)
- BBC News (2006) 'Oyster data is 'new police tool'' *BBC News 13 March 2006*.  
[news.bbc.co.uk/1/hi/england/london/4800490.stm](http://news.bbc.co.uk/1/hi/england/london/4800490.stm) (accessed 30 June 2010)
- BBC News (2006) 'Pledge to catch lawyer's killers' *BBC News 17 January 2006*  
[news.bbc.co.uk/1/hi/england/london/4619844.stm](http://news.bbc.co.uk/1/hi/england/london/4619844.stm) (accessed 30 June 2010)
- British Medical Association 'Confidentiality and disclosure of health information tool kit', December 2009 – available at  
[www.bma.org.uk/ethics/confidentiality/confidentialitytoolkit.jsp](http://www.bma.org.uk/ethics/confidentiality/confidentialitytoolkit.jsp) (accessed 1 July 2010)
- British Medical Association Ethics Department (2007) 'Guidance on secondary uses of patient information' *British Medical Association*  
[www.bma.org.uk/ethics/confidentiality/SecondaryUses.jsp](http://www.bma.org.uk/ethics/confidentiality/SecondaryUses.jsp) (accessed 20 July 2010)
- Booth, N (2003) 'Editorial: Sharing patient information electronically throughout the NHS' 327 *British Medical Journal* 114
- Caldicott Report (1997) *Report on the Review of Patient-Identifiable Information* (London DoH)
- Central Lancashire Primary Care Trust (undated) 'Data Protection and Confidentiality Procedures and Guidelines for Staff'  
[www.centrallancashire.nhs.uk/.../DATA%20PROTECTION%20AND%20CONFIDENTIALITY.pdf](http://www.centrallancashire.nhs.uk/.../DATA%20PROTECTION%20AND%20CONFIDENTIALITY.pdf) (accessed 20 July 2010)
- Davies, C and Collins, R (2006) 'Balancing potential risks and benefits of using confidential data' 333 *British Medical Journal* 349.
- Department of Health (2010) 'Caldicott Guardian Manual' *Ident code 301463*  
[http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_114509](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_114509) (accessed 10 July 2010)
- Dolan, B (2004) 'Medical records: Disclosing confidential clinical information' 28 *Psychiatric Bulletin* 53
- Durham, N (2010) "GMC website advises when to breach patient confidentiality" *Healthcarerepublic.com* 9 July 2010 available at  
<http://www.healthcarerepublic.com/search/news/1015078/GMC-website->

[advises-when-breach-patient-confidentiality/?DCMP=ILC-SEARCH](#) (accessed 23 July 2010)

Eastern and Coastal Kent NHS (2009) 'Procedure for Information Sharing with the Police' *DPCP06/CC version 1.1*

GMC (2009) 'Confidentiality' Guidance for Doctors available at [www.gmc-uk.org/guidance/ethical\\_guidance/confidentiality.asp](http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp) (accessed 1 July 2010)

Guardian (2006) 'Oyster data use rises in crime clampdown' *Guardian newspaper* 13 March 2006  
[www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation](http://www.guardian.co.uk/technology/2006/mar/13/news.freedomofinformation)  
(accessed 30 June 2010)

Hampshire Community Healthcare (2009) 'Disclosure of Information to the Police Procedure' *COR/GOV.16/VI.00*

Haynes, C, Cook, G and Jones, M (2007) 'Legal and ethical considerations in processing patient –identifiable data without patient consent: lessons learnt from developing a disease register' 33 *J Med Ethics* 302

Hepple, B (2009) 'Forensic databases: implications of the cases of S and Marper' 49(2) *Medicine, Science and the Law* 77

Humber Mental Health Trust (2008) 'Disclosing Information to the Police, Operational procedure'. *VI.10 June 2008*  
<http://www.erypct.nhs.uk/upload/HERHIS/Humber%20Mental%20Health/Corporate%20Policies/Disclosing%20information%20to%20the%20Police.pdf>  
(accessed 20 July 2010)

ICO Press Release (2010) *Poor Data Security in the NHS* 15 June 2010  
[http://www.ico.gov.uk/news/press\\_releases.aspx](http://www.ico.gov.uk/news/press_releases.aspx) (accessed 23 July 2010)

ICO Press Release (2009) *NHS Puts Records at Risk*, 15 July 2009  
[http://www.ico.gov.uk/news/press\\_releases.aspx?year=2009](http://www.ico.gov.uk/news/press_releases.aspx?year=2009) (accessed 23 July 2010)

Kalra, D, Gertz, R, Singleton, P and Inskip, H (2006) 'Confidentiality of personal health information used for research' 333 *British Medical Journal* 196

Kent Police (2010) Freedom of Information request reference 1370/2010 response of 23 March 2010

Lowrance, W (2002) *Learning from Experience: Privacy and Secondary Use of Data in Health Research*. London: Nuffield Trust

Metropolitan Police Service (2010) Freedom of Information Request reference 2010020005650, response of 22 March 2010

National Cancer Information Service – United Kingdom Association of Cancer Registries [www.ukacr.org](http://www.ukacr.org) (accessed 27 April 2010).

NHS Code of Practice (2003) *Confidentiality* (London DoH)

NHS Direct (2009) 'NHS Direct: Confidentiality Policy' *version 1*  
[www.nhsdirect.nhs.uk/.../OurPoliciesAndProcedures/ConductOfBusinessAndTheProvisionOfNHSDirectServices/030309](http://www.nhsdirect.nhs.uk/.../OurPoliciesAndProcedures/ConductOfBusinessAndTheProvisionOfNHSDirectServices/030309) (accessed 20 July 2010)

NHS Eastern and Coastal PCT (2009) *Procedure for information sharing with the Police DPC (P06/CC)*.

NHS Information Centre (2010) Freedom of Information request reference NIC-39588-6W3GX, response 23 March 2010

NIGB and ECC Terms of Reference available [www.nigb.nhs.uk/ecc/about](http://www.nigb.nhs.uk/ecc/about) (accessed 28 April 2010)

NIGB ECC applications and guidance information - [www.nigb.nhs.uk/ecc/applications](http://www.nigb.nhs.uk/ecc/applications), (accessed 28 April 2010)

Stone, M, Redsell, S and Ling, J (2005) 'Sharing patient data: competing demands of privacy, trust and research in primary care' 55 *British Journal of General Practice* 783

Second Report (2009) 'Surveillance: Citizen and the State' *Second Report House of Lords Select Committee on the Constitution*. Session 2008-2009 [www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm](http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm)

Transport for London – Freedom of Information request TfL 90319, response received 19 May 2009. Available at [www.tfl.gov.uk/foi/14883.aspx](http://www.tfl.gov.uk/foi/14883.aspx) (accessed 30 June 2010)

Transport for London, Oyster card terms and conditions – available at [www.tfl.gov.uk/termsandconditions/12321.aspx](http://www.tfl.gov.uk/termsandconditions/12321.aspx), (accessed 1 July 2010)

UK Council of Caldicott Guardians (2007) *The Caldicott Guardian; The newsletter for the Caldicott Community*, Edition 11 July

UK Council of Caldicott Guardians (2008) *The Caldicott Guardian; The newsletter for the Caldicott Community*, Edition 9 November

UK Council of Caldicott Guardians (2009) *The Caldicott Guardian; The newsletter for the Caldicott Community*, Edition 6 November

UK Council of Caldicott Guardians (2009) *The Caldicott Guardian; The newsletter for the Caldicott Community*, Edition 12 November

Wheeler, B (2008) 'Who is Looking at your Medical Records?' *BBC News 5 December 2008* [news.bbc.co.uk/1/hi/uk\\_politics/7749879.stm](http://news.bbc.co.uk/1/hi/uk_politics/7749879.stm) (accessed 30 June 2010)

Wong, R (2008) 'Assessing the Status of Medical Information in the light of the UK Data Protection Act 1998' [2008] 5 *Web JCLI*