A modern Lloyd George Envelope: CLASSIFIED when complete

When civil servants write an internal memo, it is 'protectively marked' by having the label "OFFICIAL" printed at the top[1]. This means it is covered by the Official Secrets Act and, depending on its contents, you can go to prison if you leak it. GPs have long operated the concept of a 'Lloyd George envelope'[2] for holding patient medical records, under protections that date back to 1910.

Protections that are at risk of being forgotten or ignored in the rush to a digital world.

The entire nation's detailed medical records are instead left to the vagaries of the Data Protection Act, for which the penalties for breaking are trivial by comparison. Which needs better protection – official memos, police witness statements, or all of our medical records?

The secrets you confide to your doctor should be protected at least as well as witness statements you make to the police, which you can expect to become public in due course. Police witness statements[3] in the UK are made on forms marked "RESTRICTED (when complete)".

Canada does something similar, but in Canada the rules apply to medical records as well. As a result, Canada insisted that the NSA remove names and other identifiers from the medical data of Canadian citizens that were hoovered up by its worldwide network[4]; GCHQ did not.

No change in the law is required to bring Britain into line with Canada – to move Britain from having almost no protection for medical privacy, to having very strong protection. It is a simple classification decision that can be made by the Secretary of State, in line with Government-wide security policy.[5]

We urge the Secretary of State to adopt the Canadian standard in the UK, and make a clear and binding public statement covering the following two areas:

1) Direct Care

People handling classified information need clearance to do so. It is already the case that people working in healthcare, such as doctors, nurses and orderlies, are required to have DBS checks[6]. It must be made clear that fitness to practice will carry with it a clearance to access such information as well. The Department of Health must work with the Cabinet Office and other

---

[1] https://www.gov.uk/government/publications/government-security-classifications

[2] 'Lloyd George envelopes' were introduced to resolve issues around ownership of medical records: the State provided the stationery, the doctor provided the ink and was guardian of the record until the patient died, at which point the stationery became the property of the State again.

[3] e.g. http://www.met.police.uk/foi/pdfs/disclosure_2012/feb_2012/2012020000618.pdf

[4] 'Australian spy agency offered to share data about ordinary citizens', Guardian, 2 December 2013: http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens

[5] https://www.gov.uk/government/publications/security-policy-framework

[6] The Criminal Records Bureau (CRB) was replaced by the Disclosure and Barring Service (DBS) in 2012.

interested parties to find practical resolutions to implementation issues[7], but the impact on medical professionals and those providing direct care to patients and service users should actually be quite minimal. In a direct care context, this should do more to encourage positive culture change than impose burdensome additional processes.

Audit capabilities within the IT systems that hold medical records should (already) ensure that a good record is kept of who accessed what, and enable the reconstruction of the state of a medical record at any relevant time in the past.

2) Secondary Uses

The classification of medical records must extend to the secondary uses of medical information, where no record is made of the use of data within the primary patient record itself. To be clear, the classification would apply to any and every copy, collection or dataset of or derived from patients' medical information – and to every use of such data beyond the provision of direct care to patients.

It is welcome, for example, that the 100,000 genomes project proposes to hold data for secondary use within a 'safe haven' where all access can and will be fully audited. This must become the standard for all secondary use of individual-level data. As history has shown, mere contractual 'right to audit' offers little protection.

All audit mechanisms across the care system should feed into the production of a "Personalised Data Usage Report"[8] for patients, covering all access to their records. When breaches happen, these would still be subject to the Data Protection Act, but also measures under the Official Secrets Act and related policies that would become available due to classification.

The Confidentiality Advisory Group at the Health Research Authority would remain, in its new statutory form, as an approval body for projects, as now – with an Approved Researcher[9] approval process for individuals and organisations granted access to the safe setting at the Health and Social Care Information Centre or elsewhere.

For, just like GCHQ contractors which have access to TOP SECRET signals intelligence data, organisations collecting or processing significant aggregations of individual-level data for purposes outside of the HSCIC-controlled environment would be required to meet standards appropriate to the classification level of the data.

---

[7] The national security community may have concerns around medics from countries such as China and Iran, and so terminology may become important. These concerns will clearly have not been significant enough to prevent those individuals treating patients.

[8] https://medconfidential.org/2014/what-is-a-data-usage-report/

[9] Either as defined in Section 39 of the Statistics and Registration Services Act 2007: http://www.legislation.gov.uk/ukpga/2007/18/section/39 or an equivalent for the HSCIC Secure Data Facility.

Additional notes:
Identifiability of individuals from medical records

For example, in the Maternity dataset, the 4.1m families (women) who have more than one child[10] are at high risk of permanent individual identification, due to their children's unique birth dates and linked health events – including the birth itself, and other records. For a woman with 2 children, it is 90% likely that the pair of maternity dates will be unique to that individual; for 3, it is likely that 100% are unique. A family's children's birth dates are not secret, so the data must be protected.

Spontaneous recognition due to a "rare" medical event, or a published date/event which occurs routinely but only a small number of times per day per hospital (i.e. most medical events[11]) will increase the threat to the entire population.

In England, the 181 A&E departments[12] handling England's 386 heart attacks per day[13] each average 2 events per day which, even before other information, gives a 50% probability of spontaneous identification of a victim for whom the hospital and date of event is known – though neither of these pieces of information would be considered sensitive by themselves.

Implementation Review

Following the new Government security classification scheme introduced in April 2014, there will be no doubt be a review of the protective marking mechanism in the medium term. Such a review would form a natural review point for the effects of this proposal, and would also give citizens some role and stake in the process.

Under the 2014 UK classification model[14], we presume the the old-style marking of "RESTRICTED (when complete)" will become **"OFFICIAL-SENSITIVE when complete"**, a step up what Cabinet Office describes as the "cliff face" to "SECRET when complete" seeming unlikely.

It is not that important whether medical records are OFFICIAL, RESTRICTED, CONFIDENTIAL or indeed SECRET; what is important is that the Secretary of State makes clear that their protection is important enough to invoke proper protections, such as the Official Secrets Act, which is used for data the government cares about – rather than the Data Protection Act, which is used for data it doesn't.

medConfidential
February 2015 (updated)
coordinator@medconfidential.org

---

[10] Office of National Statistics: Statistical bulletin: Families and Households, 2013 http://www.ons.gov.uk/ons/rel/family-demography/families-and-households/2013/stb-families.html#tab-Dependent-children

[11] List of A&E Departments in England: https://www.whatdotheyknow.com/request/131933/response/325271/attach/3/Annex%20A%20Final.pdf

[12] DH count: https://www.whatdotheyknow.com/request/131933/response/325271/attach/3/Annex%20A%20Final.pdf

[13] 141,000 per year in England: https://www.bhf.org.uk/publications/statistics/cardiovascular-disease-statistics-2014

[14] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/ Security_Policy_Framework_-_web_-_April_2014.pdf and https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf