Citizen Jury:
To what extent should patients control access to patient records?

Sam Smith
coordinator@medconfidential.org

What do we do?

Every data flow should be:

- **Consensual**

- **Safe**

- **Transparent**

This is how we look at everything. So if you want to have a nap, you've got the key points.

{extend on all 3. not covering safe here - don't leave papers on trains etc. Safely in theory? Safely in practice?}

Who am I?

Background in data & social science academic research

Data and technology

medConfidential
KEEP MY SECRETS

3

I was a data person working in a research group for a decade. First in academia, then at Privacy International, and for the last 2 and a bit years, at medconfidential.

We all like research. This is a research project after all. You could have said no, and you can change your mind (but Malcolm would appreciate if it you didn't) at any time.

The thing about consent for data, is when it's gone, it's gone. it's hard to get back.

What is the data?

- **linked - by the NHS number**

- **lifetime - from birth to death**

- **detailed - everything in between**

medConfidential
KEEP MY SECRETS

just to recover things you've probably been told already.

{maternity/birthday problem; 2 birthdays; 90% likely identification; 3 birthdays, effectively unique}. Particular conditions for various reasons.

Why should data be confidential?

- You

- Your family

- Your community

- Specific risk groups

Who decides what others know?

How much of the record is shown?

Gossip. Who trusts their GP not to gossip? Who trusts their GP receptionist not to gossip?

Nick Clegg's wife Miriam Gonzalez Durantez breaks elbow in fall

PA, David Hughes | Monday 26 April 2010 |

Election 2010. Nothing else happened that day, so every newspaper wrote about how Mrs Clegg fell over, and there were lots of press articles about it and the hospital, as nothing else happened that day.

How many 42 year old women broke their elbow in that way on that date in that hospital? Linked, lifetime, medical history.

The Telegraph

Tearful DJ apologises for prank call which led to nurse's suicide

DJ Melanie Greig tells family of nurse who hanged herself after prank call to Duchess of Cambridge's hospital: "I am truly sorry, I've wanted to say that for so long"

{harms - this is a fully linked dataset. It's an information problem.}

It's everything in your medical history. Whose choice is that?

Are there things your wife wouldn't want you to know?

Are there things you don't want your ex-husband to know?

Critically, what about the gossipy neighbour two doors down who works for the organisations you're dealing with.

Consent choices

- **Medical treatment is only given with your informed consent. You can always say no.**

- **implied consent for data?**

Opt out: "Do the right thing"

- **"implied consent"**

- **opt out is the current basis**

- **opt in? to what?**

medConfidential
KEEP MY SECRETS

There are often two worlds "Opt in" and "Opt out"

An "opt out" model is where there's a decision on what the "right thing" is, everyone gets told, which the ICO talked about yesterday, and those who disagree can "opt out".

Research example: pharma journalists, domestic abuse survivors

Opt in, is opting in to a specific list of specified things. This is how surgery is done - you give informed consent to a particular thing. However, "opt in" for data for the very long term is hard. How do you write that so it's understandable, specific, and sustainable?

Research and NHS management

- **Will take as much data as they can have.**

- **Will always want more.**

medConfidential
KEEP MY SECRETS

The data is never enough. If it was, it wouldn't be research or micromanagement.

Research ethics: only do research on people willing to be researched.

If you get the question right, 98% of people are happy to help. Just like you are.

Commercial use

- **Commercial use is use of data by commercial entities for their benefit**

medConfidential
KEEP MY SECRETS

What about commercial use?

You have 2 commercial uses on your list

Commercial **Re-use**

- **Commercial reuse is the onward sale of data by commercial entities to other commercial entities**

the two entities on your list might also be "re-use". Given the middlemen and intermediaries in both industries, the data may not go to a pharma or insurance company, they may go to a company working with them. "Data brokers" if you will.

Decommissioning

- Consent?

- Individual level records?

On NHS management, should individual level data be used for what the NHS calls "decommissioning"? (that's closing hospitals). How would that work in an opt in or your opt out world?

There are some things individual level data shouldn't be used for — those purposes are met with aggregated statistics, counts, averages, not individual data. Your first point is about funding decisions — has a case been made that they require **individual** level data? Or do they just need to know summaries, averages, "people being treated for this condition in this hospital do 10% better than that one?". Creating the statistics requires individual level data, but the statistics are published, in the same way statistics on the economy are published, but your bank statement isn't.

How much do you want to know?

Currently, how your personal medical record is used is secret.

All of the scenarios you've been asked to consider might happen. None of them might. You don't know.

Should you know how individual level data about you has been used?

Experience

it's shorthand to say that opportunities get used by "fraudsters and charlatans" first.

There's an NHS Pharmacy called Pharmacy2U, they're an internet chemist, which do prescriptions over the web, and will sell you little blue pills, apparently discreetly.

Then the ICO found out that they sold the names and addresses of their customers without telling them.

Whether they should have done that is not our concern.

It's who was at the front of the queue that's most of interest, and what they wanted. They weren't marketing things to 20 somethings buying little blue pills.

They were marketing to people who were elderly, who were less congnitively aware.

One was selling herbal replacements for the prescriptions they'd just bought. They didn't work, but they were expensive.

Another was running a lottery scam, going after life savings.

The people targeted when data gets sold are the elderly, the less cognitively aware.

And if you think that doesn't affect you, if your mother in law loses her life savings due to a scam, where's she going to live? ;)

Predicting the future

the framework has to work into the future.

The job of the NHS is to save lives.

Whatever happens, the decisions you take have to work for everyone. Those keen for their data to be shared, and those who have good reasons for it not to be.

Questions

Every data flow should be:

- **Consensual**

- **Safe**

- **Transparent**

Questions?