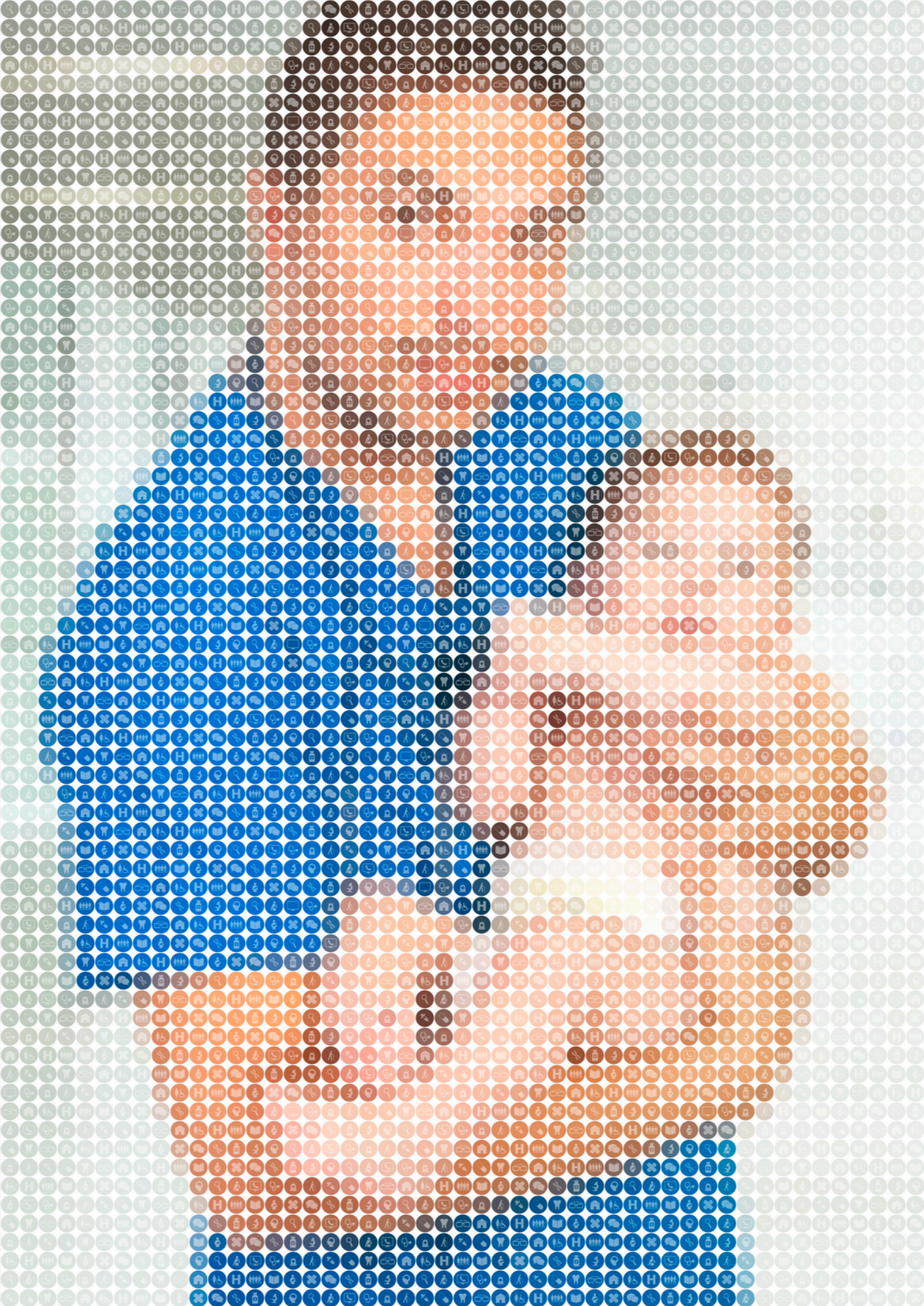
Confidentiality in a digital world: Deliverable, but not yet delivered

August 2017



Welcome

medConfidential works to ensure every flow and use of patients' data in the NHS and beyond is consensual, safe, and transparent. As of summer 2017, after the Government's response to Caldicott 3, but before the Data Lake starts leaking, we summarise the current positions – and where things may be going, depending on future choices.

The effects of an uncontrolled publication of the nation's identifiable consolidated hospital treatment history remain unclear, even if the data is only "anonymised in line with the ICO's Code of Practice". The initial response will likely be woefully inadequate – as denial of the existence of any potential problem still persists. That those who didn't opt out were put at risk will be bad enough; that people who explicitly chose not to accept that risk were also exposed will be catastrophic for trust in the NHS and Government itself.

The publication of the Government's response to Caldicott 3, however, demonstrates a new commitment to transparency to patients. Promises only begin to be delivered in 2018, so transparency may yet be sacrificed in a dark corner.

There are other reasons for hope.

The Chief Medical Officer's Annual Report, published earlier this year, shows that based on patient consent and following medical ethics, both innovative research and novel methods of care remain entirely feasible. Those in commerce and research who see patients only as as 'rows in a dataset' may well continue to dismiss consent as a hindrance – but doing so is their unethical choice, not a necessity.

The ongoing fiasco that is the National Data Lake / 'regional data ponds' / interoperable regional innovation hubs / care.data 2 shows that NHS England is capable of ignoring every hard-won lesson; just as some other bodies chose to. The ongoing failings of PHE's Cancer Registry derive from the same culture that created care.data.

Supported by the enlightened long-term perspective of our funders, the Joseph Rowntree Reform Trust Ltd, we are measured solely on progress towards making every flow of patient data in the NHS be consensual, safe, and transparent. Unlike others, medConfidential is not distracted by membership bonuses (we don't have members), headlines (we can't afford media monitoring), or column inches (a legacy of a bygone age). Whether any particular individual opts out or not is a decision for them – our goal is that every patient has the factual information necessary to make an informed decision that is correct for them and their family.

To those who choose to deny patients that choice, medConfidential will repeat the lessons that should have been learnt from care.data. While we would prefer institutional learning and culture change to have made that unnecessary, those choices are out of our hands.

There should not be, as some would have it, a battle between privacy ***or*** innovation. To move forwards, the ultimate arbiters of how their medical records are used should be patients; each patient having the information they need to make the choices they have under the law.

In the much longer term, win or lose on any particular battle, we still have hope that people can count on public bodies to do the right thing… even if they may try everything else first.

medConfidential
August 2017

NHS in England

medConfidential was founded in response to loopholes in the Health & Social Care Act that enabled NHS England's care.data project – foreseeing the trainwreck it turned out to be.

care.data exposed the rot that had set in with the handling of patient records, and – to their credit – the Department of Health and Secretary of State took steps to try to resolve it, without a body count or a monument to neglect.

HSCIC (now NHS Digital) commissioned the Partridge Review to examine how it should move forwards. The Review's findings remain sound; although its recommendations are only partially delivered.

While NHS England has often been part of the problem over the last 4 years, it is rarely part of the solution. And as the Department of Health makes public promises to patients, NHS England actively ignores any parts they feel are politically inexpedient (for them). Where officials could have stepped up, they instead drown themselves in their own Data Lake.

Departmental thinking is naturally refreshed by a General Election or a reshuffle; out in the wilderness, NHS England's Data Lake shows its thinking is the same as when it began.

There is an oft-stated belief that using Electronic Health Records, and flowing data along a care pathway, improves care and leads to better outcomes. But why does this belief not translate into measurement and transparency to patients? And why not into the Payment By Results finances? While NHS England implements the priorities of the Secretary of State, its only lever is funding priorities – which, in this case, it chooses not to use.[1]

The commitment from the Department of Health to send a letter describing the new system to every patient who has opted out is vital for confidence in the Caldicott Consent Choice for the 1.2m people who have already expressed their dissent. However, it remains unclear what the vast majority of people – who didn't go through the multiple steps of opting out will know. Every patient must know what their choices are, and receive a letter outlining the new system; the "fair processing" requirement. NHS England may wish to build a Data Lake, but if it becomes polluted, the public must know what it is they are choosing.

The politics of NHS England are such that decisions tend to be taken in dark corners, where officials hope no one can notice. How they choose to take decisions is a matter for them and their accountability mechanisms. But if patients will know how their records are used, then such secrecy is unsustainable. Will the Department of Health and NHS Digital protect them?

Based on foundations laid by Jeremy Hunt during his time as Secretary of State, there is a promise that, in future, patients can know how their records have been used. This will have many diverse consequences, most of them ultimately positive.

There are a number of organisations that see the opportunities of privacy ***and*** innovation, but in the shorter term, at the other end of the spectrum, the list of loopholes emerging covers the breadth of organisations (and subsets thereof) that believe the rules don't apply to them.

---

[1] https://medconfidential.org/2017/any-data-lake-will-fail-and-sir-humphrey-knows-this/

Following the Government's response to Caldicott 3, this is the current state of play:

	Consensual	**Safe**	**Transparent**
GPs - Direct Care	✔	✔	✔
GPs - local CCGs / councils	✔	Varies by recipient	Depends on GP
GPs - research copies	✔	Unknown	✘
Hospital - Direct Care	✔	✔	✔
Hospital - local sharing	By 2020	Varies by recipient	By 2020?
NHS Digital: SCR controls	✔	✔	In 2018
NHS Digital: Safe Setting	✔	✔	✔
NHS Digital: Sale of hospital records	✘ (opt outs ignored)	✘	Partial: now; More: late 2017; Full: Late 2018.
NHS Digital: Commercial reuse of hospital records	✘ (opt outs ignored)	✘	✘
NHS England: CSUs / councils / national	Variable	Unlikely	✘
DH family:			
PHE disease registries	✘ (no fair processing) ✘ (misleads patients)	✘	✘ (proposed as a postcode lottery)
CPRD @ MHRA	✔ (Type 1)	✘	Partial (unknown: will it be included in the NHS lists?)
Genomics England	✔	✔	✔
Chief Medical Officer 2017 Annual Report plan for Cancer care	✔	✔	✔

A longer and current version of this scorecard is available at medconfidential.org

Patients as a bargaining chip - Public Health England & beyond

PHE's approach to the cancer registry is emblematic of the deceitful paternalistic approach to data copying that was the worst of care.data's failings. Such an approach cannot survive the introduction of GDPR in May 2018.

PHE has the opportunity to deliver a consensual, safe, and transparent disease registry infrastructure – integrating more data for patients and research, and doing so in a manner that is lawful. But it cannot do so by selling the data out the back door to avoid the rules.

Public Health is an unfortunately neglected part of the DH portfolio. Prevention is far cheaper than cure, yet the failures of data handling at PHE are unchanged since a highly critical report from The National Archives' Office of Public Sector Information in 2015.

The items PHE chooses to omit from its Data Release Register demonstrate how far is left to go before PHE recognises – let alone corrects – failures that, in the NHS, precipitated the suspension of data releases, and then later, Caldicott 3. The Cancer Registry (like the Data Lake) represents the path not travelled, after care.data's failures had become apparent.

Dumping the burden onto the patient, not the system, is unsustainable. It can be ignored by the current inhabitants of certain roles – they do not expect to be responsible when the programme collapses, and so they may as well make their life easier.

Cronyism in non-NHS data access

Patients should be able to see where their data was used. Whether CPRD (from MHRA), QResearch (from EMIS), TPP ResearchOne, SHIP, SAIL, or commercial reuse licensees, each should be required to meet the transparency standards of NHS Digital. Patients should not have to puzzle out why their data gets copied where; they should be able to see.

The Haldane principle is vital to continued public confidence in the special nature of academic research. Irrespective of whether the payment plan is measured in pounds or papers co-authored, data access arrangements, accessors, and public benefit should be fully transparent to the patients whose records are used as a bargaining chip.

Similarly, where NHS Digital is releasing patients' home addresses and details of their GP, while it may be lawfully compelled to do so – according to the entity doing the compelling – it is not gagged from telling those patients whose records it handed over. The MoU with the Home Office is an abomination. We note with respect that three NHS Digital Board members who had raised questions over the NBO's actions are no longer members of the Board.

GDPR for GPs & Care providers

The main change in GDPR is accountability – which, for GPs and care providers, should mean a demonstration of existing accountability to your patients.

While it is mandatory, unless you've ignored advice in the past, the GDPR review process should be something akin to be the equivalent of a prescription review, as opposed to a life-changing diagnosis. For most, therefore, this will simply be a time to check that your organisation's contractors are not breaching your medical ethics obligations; in the way they should already be doing.

GPs treat patients not conditions. You are likely the only people in the health system who care about the *whole* patient, who see conflicts, and who deal with patients in person.

Changes are possible – indeed, this is your opportunity to review and correct any outstanding issues, without blame, as a consequence of the change in the law and other developments since you last had such a review. Is there anything useful that modern tools allow you to do, that wasn't possible the last time you had such a review? (The first Caldicott Report was in 1997, and the Data Protection Act came into force in 1998; a systematic and broad review may not have been done since then.)

Regarding the implementation of Caldicott 3: if you are compelled to share medical information, rather than being in the sole position of making a 'perpetually perfect' decision, the commitment from DH/NHS is that the patient should be able to see how their data is used. This includes for the purposes of research and administration; activities that would include, for example, risk stratification.

You may also in coming months receive many pitches for GDPR consultancy. Who you pick is up to you, but there are some simple credibility tests: do they follow *current* (i.e. 1998) law – are they registered with the ICO, for example, and *when* did they register? What are their medical credentials?

For your patients, this process, and the communications around the national opt-out mechanism coming from March 2018, are an opportunity to move people to potentially cheaper and – when correctly implemented – safer mechanisms online. The change in the law will allow you to embed *current* best practice, and (should it prove necessary, or politic) to be able to lay responsibility for changes on "the EU"…

The system is learning:

The future of Genomic Medicine

The potential of the Chief Medical Officer's Annual Report on the future of genomics in the NHS is based on patients' consent, and on research. It demonstrates a core tenet of medConfidential: that there need be no conflict between good research, good ethics and good medical care. Properly implemented as the future of consensual, safe, and transparent genomic medicine, it could be a roadmap.

Despite these promises, there are still some who believe patient consent is unsustainable; people who believe in a short-term rush to sequence everyone once, from baby blood spots if necessary. They are not only shortsighted, but wrong – and misunderstand the basis of medical ethics. (hey are also generally not medics but technologists, or those with financial or other interests.) The Chief Medical Office's Report lays out why this is unnecessary: you can ask patients, and gain consent. The consent model of Caldicott 3 can include genomics, and AI, and also whatever comes after genomics and AI.

Caldicott 3

Problems around the consensual, safe, and transparent use of data in the NHS are not new. They predate care.data, NHS England and even the first Caldicott Report, in 1997.

The appointment of a National Data Guardian for Health and Social Care in late 2014 was an important step.

The appointment of Dame Fiona Caldicott as the first National Data Guardian gave the post continuity from the Independent Information Governance Oversight Panel and, before that, the statutory NIGB.

Dame Fiona and her Panel have a long heritage of ensuring that patients' data is used safely to help patient care. medConfidential remains confident that existing and ongoing challenges to the consensual, transparent use of medical records can be met by those working towards the practical implementation of the Caldicott Consent Choice.

We welcome and support the cross-party commitment, restated by this Government, to place the National Data Guardian on a statutory footing.

Safe Settings and risks from data

Safe settings were a key recommendation of the Partridge Review:[2]

> "That the HSCIC actively pursues a technical solution to allow access to data, without the need to release data out of the HSCIC to external organisations."

medConfidential pointed to safe settings, using the example of the ONS Virtual Microdata Laboratory, the very first time we gave evidence to Parliament. It is the combination of safe institutions, safe people, safe projects, safe settings and safe outputs that keeps even the most sensitive data safe – as others have since gone on to prove.

It is the very details and characteristics within individual-level, linked lifetime health histories that make them so useful, and valuable, and at the same time so sensitive and identifiable. Yet many risks of reidentification and data loss (as well as other cybersecurity incidents) can be mitigated entirely with the use of a safe setting, and even 'high-risk' data can be analysed in a way that is comprehensively monitored.

Across the NHS, permanently and uniquely identifiable individuals arise every day – the "Ebola nurse". Each requires protection that can only occur within a safe setting, or by 'damaging' the data. Similarly, the dates of maternity events constitute special unique identifiers for a vast swathe of the population, based on the fact that birthdates of a family's children are not entirely secret. This is the reality of the rich but fundamentally identifiable data the NHS accumulates and uses as it delivers health care; data from which we could all benefit and learn.

Genomics England's successful use of a safe setting shows the model works for innovative research, where there is the will to do so. The benefits of a safe setting include being able to use much richer and more detailed linked data – given many concerns about safety are handled by the setting and the processes and procedures around it,[3] not the dataset or the researcher. And, with full transparency and positive feedback, the trustworthiness of the shared endeavour can be established from a basis of knowledge.

One cannot merely assume or assert trust; it has to be earned. And with the transparency promised by Government, a clearly communicated and meaningful Caldicott Consent Choice – respected by all, across the entire system – and safe settings, the NHS has within its grasp the basis for trust into the 21st century.

---

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/367788/Sir_Nick_Partridge_s_summary_of_the_review.pdf

[3] https://blog.ons.gov.uk/2017/01/27/the-five-safes-data-privacy-at-ons/

The Private Sector

There is wide variation in data practices within the private sector. The gamut of intent is spread across the full spectrum – from organisations that will try to make a quick buck off anyone gullible enough to give up their password for a chocolate bar, to those with a long-term commitment to sustainability and public trust.

Many of the private suppliers to the NHS are already capable of meeting the requirement to be consensual, safe, and transparent. Indeed, as the Government's response to Caldicott 3 noted, GP IT providers TPP were the first to deliver transparency over out-of-surgery access to GP records, followed by EMIS. Each for their own reasons, they began to deliver what was necessary ahead of the requirement to do so; both companies acting as responsible data processors.

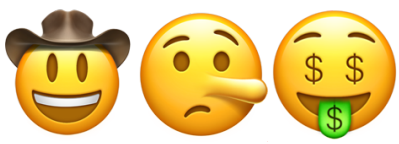
In the opposite corner there is Google DeepMind, which took 1.6 million patient records in an unlawful deal, and refuses to delete them. Claims to transparency and ethics have to be matched by actions. If you claim you publish everything and then "accidentally" omit the one page from the contract that shows the controversial data being copied remains being copied, it is dishonest to refuse to restore it.

The profit motive drives a tendency to spin the benefits, play down risks, and externalise the costs.

In the world of Data Protection, the most recent clear example of the failures of the market is the "cookie law"; that annoying banner you have to click through on lots of websites. While the ICO and others provided a single compliant design, given its annoyance, they were legitimately expecting it to be iterated and improved in the market. This did not happen. The 'lowest common denominator' became the commercial default choice. (There is still scope for iterative improvements, but no one wishes to spend the effort to design them.).

Similarly YouTube, with its *-nocookie* domain variant, has not taken off – even in privacy circles. It does what was asked for, yet almost no one asking for it actually uses it; even the ICO's own YouTube embeds do not. Getting this right requires effort.

As the Information Commissioner said in her first speech, it is not privacy or innovation, but privacy ***and*** innovation.



Artificial Intelligence

There is a great deal of focus on “AI safety”, often used as a catch-all term for issues the AI companies would like to convince you are not problems – though if they are, then they have them all under control.

From ‘super-AIs’ going rogue and taking over the power grid to secret languages, whatever else it does, AI safety must also include accountability. Simply put: what data was fed to an AI, and why? To do “AI safely”, records must be kept of what data went where, and when. For without accountability there cannot be safety, and neither can there be confidence in safety.

medConfidential does not take a position on AI research *per se*; the existing ethical research processes should be sufficient for AI, assuming the rules for research are followed. This may require more paperwork than using freely-published open data, but if as an organisation you are committed to properly handling patients’ records, the least you should do is fill in the paperwork that binds you to that promise.

It is striking that DeepMind is more effectively held to account for how it treats Google’s internal data, than it is for how it handles NHS patient records.

It remains the case that Google DeepMind – whose project with a large London hospital was unlawful – while it claims transparency, “accidentally” omitted (and still refuses to publish) the list of data it continues to receive under the Data Sharing Agreement that it wrote. This would be of concern, even if it wasn’t also public that DeepMind is processing data outside of that agreement with *no* lawful basis.[4]

AI could be integrated into the NHS safely, to aid clinicians and their patients, without mandating a monopoly. The latter is, however, a commercial choice – not an ethical one.

The Partnership on AI make claims, but will they be backed up by actions? Experts are working on how to build an AI safely. But safety and public confidence in AI requires that *every* use of (health) data be consensual, safe, and transparent – whether AI or not.

It remains unclear what first attracted Google DeepMind to unlawfully process 1.6 million medical records in secret. But the truth always comes out…

[4] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

Data in the Rest of Government

Using ‘digital’ to transform the relationship between the citizen and state was in the Government’s Spring 2017 Manifesto. There is an easy place to start: where a citizen interacts with a digital service, and where administrative decisions are recorded, the digital service should make the administrative record of the decisions visible to the citizen.

The Manifesto was very clear on the potential for digital services, based around GOV.UK Verify, to transform the relationship between citizen and state – but such transformation requires accountability of the State to the citizen.

When DWP and GDS were creating the Universal Credit interface, there was originally an audit trail of which JobCentre roles had accessed the record and why; the claimant and staff could see each others’ actions. DWP civil servants insisted the staff audit trails be removed before ministers saw them – it would be embarrassing were claimants to be given evidence of how decisions were made. So instead, we’ve had more years of DWP’s toxic and secret failings dripping into the public domain, where “business needs” are prioritised over the public interest.

Government will treat any data on citizens as its own, and feel entitled to do with it entirely as it wishes; the Home Office fear of anything has become a fear of everything. Government can choose to be transparent, or it could choose to hide every action behind the veil of secrecy. The Digital Economy Act 2017 does not require transparency when data is copied, nor does it prohibit medical records being copied at the whim of a civil servant who can write down a reason.

Digital tools can transform the relationship between citizen and state for the better. When civil servants approve access to data, the case they make should be published – with a record visible to all those citizens whose data was accessed. When the data was from a service which has a digital tool (which would include everyone on Universal Credit) that mechanism is readily available. It all comes down to political will *vs* “business needs”.

It is unrealistic for citizens to rely on every civil servant to always make the right choice about data for every citizen. Even if most do, institutional cultures mean it may be a choice between the right choice for citizens, and the other choice that gets them promoted.. When the Cabinet Office told the NHS that Government wanted access to GP patient records so the Home Office could look for fraudulent marriages in the sexual dysfunction data, for example, they were laughed out of the room. That is possible only in such clear and egregiously misguided cases.

The political will of the Manifesto was clear. However, in the dark corners of Whitehall, the civil service machine sleeps content in the knowledge it is the politicians who will be held accountable by the public. But a political quiet life is wholly dependent on no civil servant ever having a perverse incentive and making the wrong decision. Our experience of the NHS and rest of Government shows, this happens routinely. In a digital world, the current culture of cover up is not entirely wise.

Local Government

Local Government can already, with citizen consent, access data necessary to provide the services needed by that citizen.

However, local authorities continue to fund lobbyists to write reports advocating that medical records are handed *en masse* to local authorities. Without knowledge or consent, such access will regularly feed gossip and prejudice decisions about local people in ways the lobbyists deny would happen. Such expensive and glossy reports will keep being piled up until they stack as high as the buildings in which some residents live.

Lobbyists attempt to reassure, saying such organisations only ever act “in their residents’ best interests”.

The surviving residents of Grenfell Tower might take a different view.

Left: Grenfell Tower smoke over central London.
Photos: Camden New Journal

We would like to thank:

- Gus, Andy, Fleur, Terri, for agreeing to create medConfidential;
- Joseph Rowntree Reform Trust Ltd Directors, Trustees, and Staff,

- Secretary of State Jeremy Hunt, Ed Jones, Katie Farrington, David Knight, and teams;
- Ciarán Devane as the chair of CDAG1, alongside Understanding Patient Data at the Wellcome Trust, AMRC, BHF, BMA, Cancer Research UK, Macmillan, MRC;
- Dame Fiona Caldicott, the NDG Panel, and Office;
- In HSCIC, Andy Williams and team, especially Caldicott Guardian Prof Severs and teams, Sir Nick Partridge, Eve Roodhouse;
- Jeni Tennison, Gavin Starks, Kathryn Corrick, Ellen Broad, Peter Wells, Amanda Smith et al at the Open Data Institute - they saw the potential of data accountability before 2014;
- Liam Maxwell and team, including Matthew Gould;
- Mustafa Suleyman, Ben Laurie, Verity Harding and teams for contributions through the megaphone of Google DeepMind;
- NHS England's care.data programme for the images on page 2 & 15;
- Nick Pickles, Renate Samson, Dan Nesbitt, and Jim at BBW, ORG, et al;
- Rachel Coldicutt, Janet Hughes, and everyone at dotEveryone;
- Sarah Gold, Richard Pope, and the team at Projects By IF;
- TPP and EMIS;
- Use My Data, and Chris Carrigan for encouraging the detailed look at Public Health England;

- Mike Bracken, Tom Loosemore, Janet Hughes, Richard Pope, et al, at GDS who made this possible by showing a better thing, and delivering;
- Tim Kelsey, Paul Maltby, Kevin Cunnington, and Wills Cavendish & Smart, each for their own alternate approach which was also illustrative,

and last, but certainly not least, the list of people whose contributions were too important to omit, but remain too sensitive to mention.

You know who you are, even if others can not... Especially *you*

Thanks,

From Phil & Sam, with our Board, supporters,
and all patients who can now make more informed choices.

WHEN WE CAN SEE WHAT'S HAPPENING, WE CAN MAKE THINGS BETTER

CONNECTING INFORMATION FOR THE HEALTH OF THE NATION

medConfidential is an independent non-partisan organisation campaigning for confidentiality and consent in health and social care, which seeks to ensure that every flow of data into, across and out of the NHS and care system is *consensual, safe, and transparent*.

Founded in January 2013, medConfidential works with patients and medics, service users and care professionals; draws advice from a network of experts in the fields of health informatics, computer security, law/ethics and privacy; and believes there need be no conflict between good research, good ethics and good medical care.

Bitcoin: 1AyjjjguLUcn5enF3LDdqLf52Se8Ydinpg
Ethereum: 0x42484C23Ca50425795B8bbb15e0DAA0BCe7Bf f5A
Zcash: t1NWtfut3k2eh5cJtFFc79LmNzDjXcD48a7

www.medConfidential.org/donations