

21 APR 2020

Easier said than done: the challenge of transparency during Covid-19

By [Natalie Banner](#), *Understanding Patient Data Lead*

The Covid-19 pandemic has seen an unprecedented demand for increased transparency from the Government. There is a strong public interest in clarity and openness of decision-making and the data behind it, from the models underpinning public health strategy, to answering critical questions about the companies involved.

It is easy to demand transparency, to expect our decision-makers to open their processes and data to public scrutiny. I firmly believe this is necessary to create a trustworthy system. But the experience of the past few weeks has taught me just how difficult it can be to do in practice, and transparency alone won't work without trusted relationships. In this post I'll set out some of the dilemmas we have navigated so far and hope to provide some useful insights to others.

Data in the Covid-19 response

Over the past few weeks, the Understanding Patient Data (UPD) team has been seeking to ensure NHS digital responses to the Covid-19 pandemic are as transparent and open to public scrutiny as possible. We've provided advice and convened people to feed in to NHSX's work on:

- [the data store](#), a potentially controversial collaboration with several international tech companies that had been subject to media scrutiny and speculation
- early plans for a contact tracing app, [based on a paper](#) by a team at Oxford
- a symptom checker app, similar to other [independent apps](#) already being promoted

For all of these, important questions need to be asked about how the collaborations were established, how data will be managed and used (especially in the longer term), the evidence base for the technologies, who is making decisions and how people will be informed.

Why is this hard?

As part of this work, we pulled together a group of people who could ask detailed questions of NHSX and scrutinise the plans as they evolved, to ensure

common public concerns could be addressed early on. The plans were developing at incredible pace through multiple teams and many competing pressures. This brought us to our first transparency dilemma:

Challenge 1: privacy vs transparency

UPD facilitated a video call at short notice, digging into our contact list for people who'd be able to help. This included the authors of a recent [open letter to NHSX](#), members of the National Data Collaborative which includes medical research charities and patient groups, and privacy campaigners.

These contacts were bcc'd into an email invite – it'd be ironic for a call on data and privacy to lead with an email displaying everyone's contact details. But this meant it was not clear who was invited or on what basis, why some, not others, and by default it excluded those UPD doesn't already have a relationship with.

Was this a failure of transparency in the interests of protecting people's privacy and details?

Challenge 2: comprehensive and complete vs quick and pragmatic

On an hour's video call with over fifty participants it would have been chaotic to have everyone speaking. As a solution, I asked people to add questions to the chat function and attempted to group them thematically, picking out questions that seemed to best represent common concerns. For example, there were several on anonymisation, accountability, procurement and the use of data for research.

However, in attempting to broadly cover the main issues I missed the nuance and technical detail from many of the individual questions, so some of the value of having expert questioning was lost. I was also inevitably selective in what I covered. The NHSX team took away the questions that we didn't get to, but in one hour there was limited opportunity to delve into the concerns in much depth. Did we lack transparency in how we managed questions? Were we too selective, resulting in the illusion of a transparent forum for discussion but a failure of in-depth scrutiny?

Challenge 3: to share or not to share

Several participants asked for copies of the slides presented. The NHSX team wanted a bit of time to respond to some of the questions or clear up confusions in the slide deck before sending.

There were good reasons for holding back; the slides represented a snapshot of thinking on 30th March, which quickly became outdated and could be misleading if they were more widely distributed or believed to represent final plans. But at the same time, failing to share the presented information could seem like bad faith or that there was something to hide. Should we have pushed harder to distribute the slides as they were presented? Was it a failure of transparency to allow them to be edited? Did this helpfully clarify key points or obfuscate what was presented?

Reflections

There is inherent vulnerability in showing working as it evolves. There are bound to be gaps, and ideas that will change or be dropped over time. Fundamentally, sharing this kind of information requires all parties to trust one another's intentions and integrity. On the part of NHSX, they needed to trust that the stakeholders on the call wanted to be critical friends in the interests of serving the public good, not to catch them out, or capitalise on mistakes for their own agendas. On the part of the stakeholders, they needed to trust that NHSX were being open and honest about their thinking, not conducting a political or media spin operation, and that their input genuinely would shape the proposals.

The push for transparency can be easily undermined when the intentions of different parties are not trusted. As we've seen from the avalanche of misinformation emerging during this pandemic, transparency over data and decisions won't help if people don't trust the integrity and motivation of their sources.

We should demand that public decision-makers are held to account and transparency is a vital component of this. At the same time, we should recognise that this involves practical trade-offs and decisions, all of which will be called into question if people's intentions and integrity aren't trusted in the first place.