Shared challenges

Across our varied discussions there were a number of issues that are often seen as common challenges. While the specific nuance may vary by region and stakeholder, these are all viewed as obstacles to be overcome. Indeed, without successfully addressing them, many felt that the wider ambitions for and opportunities from better use of patient data may well be difficult to achieve. As such, these shared challenges appear to be a current priority for many.

Integration – Although some organisations are wary of sharing valued information, several governments and markets seek new ways to merge disparate data sets for greater social benefit. As the appetite to scale and combine new sources of personal, societal and clinical information increases, the expectation is that technology will provide solutions that better bridge data gaps and ensure inter-operability in the future. Establishing common standards across data sets will be a key driver of change.

Trust – In many regions, trust needs to be (re)built between payers, providers and patients as well as with new entrants coming into the healthcare arena. New technology platforms and improving communication with the public both play a major role. Concern about ulterior motives for the use of data is high and some see AI adding to the challenge. Many recognise the need for greater transparency on practice in some pivotal areas.

Ownership vs. Access – If access to patient data is to have impact it needs to be aggregated and shared but there are concerns around ownership and who makes decisions around its use. Patients may have increasing control of their data, but whether they are its real custodians and are able to control access to it depends on culture, regulation and need. Many countries are moving towards supporting greater individual access and ownership of health data – a question will be how well citizens engage with it.

Security and Privacy – As anonymized, aggregated data is more easily re-linked and sensitive health data is a target for cyber-attacks, questions are raised around the benefits of centralized vs. decentralized data and the impact of localization. Given both the sensitivity and value of healthcare data it is little surprise that security and privacy are high on multiple agendas. As vulnerability and risk increase apace with greater focus from external hackers and internal sources, these are growing concerns for many.

Each are detailed in the following pages

Integration

Although some organisations are wary of sharing valued information, several governments and markets seek new ways to merge disparate data sets for greater social benefit. As the appetite to scale and combine new sources of personal, societal and clinical information increases, the expectation is that technology will provide solutions that better bridge data gaps and ensure interoperability in the future. Establishing common standards across data sets will be a key driver of change

Although there has been a proliferation of health data and its collection, many see that we are not yet at a point of unleashing its power because the vast majority of information remains proprietary and fragmented among insurers, providers, health record companies, government agencies, and researchers. Despite the technological integration seen in banking and other industries, healthcare data has largely remained scattered and inaccessible.[22] Indeed attempts to make hospitals and clinics more efficient by building huge, centralized IT systems have a sorry history - just look at a failed patient-record system for Britain's National Health Service, scrapped after 10 years at a cost of around £10 billion ($15 billion).

BARRIERS

Part of the difficulty is that many of today's healthcare systems are rife with multiple and legacy systems. In the US, for example, EHRs currently remain fragmented among 860 ambulatory care vendors and 270 in patient vendors. Others are similarly disjointed. IT issues such as compatibility and version control are obvious

hurdles, as is the fact that many healthcare systems are increasingly strapped for cash, which inhibits their ability to secure sustained financial support for the investment required. At some point the nettle will have to be grasped and significant investments made.

To date the global healthcare industry has largely struggled to successfully manage the myriad stakeholders, regulations, and privacy concerns required to build a fully integrated healthcare IT system.[23] The problem is clear; the Institute of Medicine sees that: *"A significant challenge to progress resides in the barriers and restrictions that derive from the treatment of medical care data as a proprietary commodity by the organisations involved... Broader access and use of healthcare data for new insights require not only fostering data system reliability and interoperability but also addressing the matter of individual data ownership and the extent to which data central to progress in health and health care should constitute a public good."*[24]

NOT SHARING

It is true that many organisations see that their data has both commercial and competitive value so the principle of sharing this more freely is not an easy conversation to have. Currently several major healthcare organisations do not share their data and see no benefit in changing, *"not with Google nor with Apple even though they are asking for it: Partly this is about ethics but also about ownership and use."* In addition to this some are wary of providing international access to patient data because of security concerns. With the rising tide of data hacks and wider cyber-security now a mainstream concern in healthcare, the idea of centralized ownership of medical records is increasingly being viewed by some as a security risk. They argue that *"we need to decentralize this data because the more it's amassed, the more likely it's going to be hacked."* Better regulation may go some way to address this conundrum and indeed a number of guidelines are being shared which set standards, but, as yet, there are few incentives for organisations or nations to deliver. Also, aside from the security and ethical issues many point out that standardizing data from the current disparate data sets is an expensive and time-consuming business. And no one has yet answered the fundamental question of *"who will pay money to clean data."*[25]

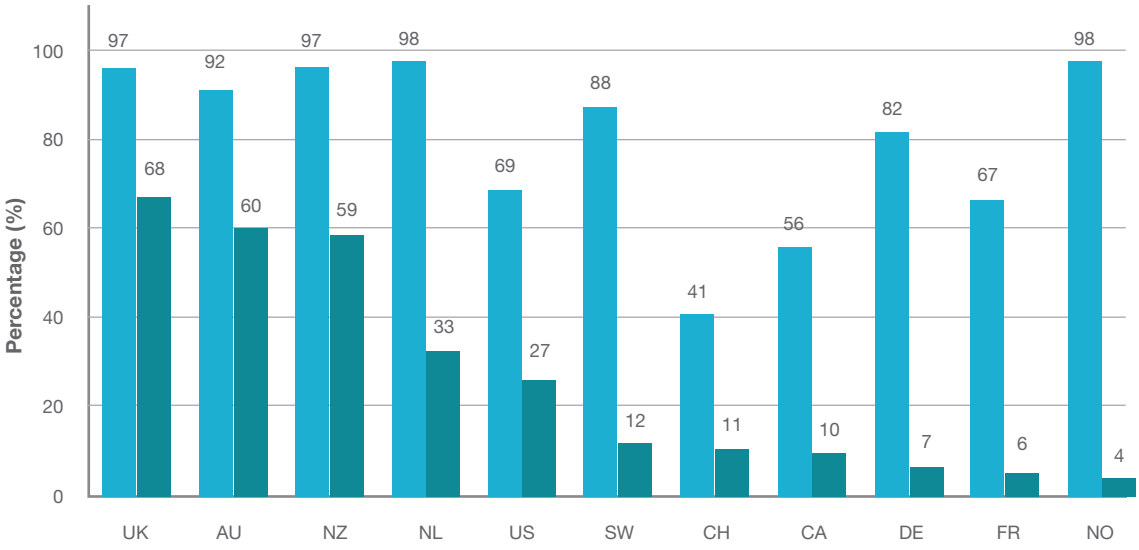
CONNECTING DATA

The technological difficulties of combining disparate sources of information into a commonly accessible format should not be underestimated. There is certainly great hope that it can be achieved with multiple organisations and governments, many under pressure from escalating costs, aspiring to an end-point where the entirety of an individual's health data is clearly presented, easily accessed, available for analysis and, at the same time, protected. Realistically this possibility, even for sophisticated healthcare services, is a few years or so away. A good number of organisations expect to be grappling with legacy systems, poor interoperability and unstructured data for quite some time to come. In the short term the ambition for many is therefore to achieve better connectivity between data sets within the clinical arena by improving harmonization, standardisation and data quality.

Beyond this there is growing recognition of the value of self-generated personal and proxy data. Although this is often more unstructured and does not meet current medical standards, it does provide a contextual richness for clinicians which helps them to better understand patient health. Many agree that more rigorous collection and analysis of this will be of great benefit and will help to shift healthcare away from treatment of conditions to one that prevents illness, *"today we have 1% wellness data and 99% clinical – in future it will be 99% wellness and 1% clinical."*

What is clear is that there is *"a tsunami of health data heading our way"* and making the best out of this relies on the ability to integrate the most useful information and make it more widely accessible. Many agree that we are generating more data than we can currently use and expect the situation will continue simply because of the impending *"data storm of information coming from millions of people."*

Doctors with EHR and Multifunctional Health IT Capacity



Source: Commonwealth Fund 2014

In Oslo, however, the view was that managing this is a temporary challenge and that by 2030 *"there will be no real barriers to combining both structured and unstructured data. There will be better quality of data, more standardization and greater harmonization."* Others were keen to point out that *"healthcare is a multi-disciplinary team sport and we need to be able to share and use insights and information more smoothly and effectively – and see the bigger picture not just a silo."*[26]

STANDARDISATION

Quite how this ambition can be achieved given the highly fragmented systems found in many countries today is not obvious. Already boasting a high-quality healthcare service, Singapore is making strong moves around multi-data set connectivity, but other countries are facing much more fundamental challenges. Irrespective of location, most workshop participants agreed that, in order to take advantage of new technologies, strategies must be developed that will align regulation, funding models and outcome-based incentives. Once a common framework is developed, the notion of a connected information set that could act as a 'personal health passport' becomes more realistic. At the moment this is the long-view, even for Singapore where our discussion focused primarily on the need for greater institutional sharing of data between government departments such as the ministries of social development, health and education. Looking ahead the ambition is that, *"by 2030, payers (both private and public) will use standardized platforms to produce and consume data. Moreover, patients will be incentivized to bring in their own data sets for aggregation to improve the ease of access to services."*

Given all this, what then are some specific technological challenges that need to be addressed?

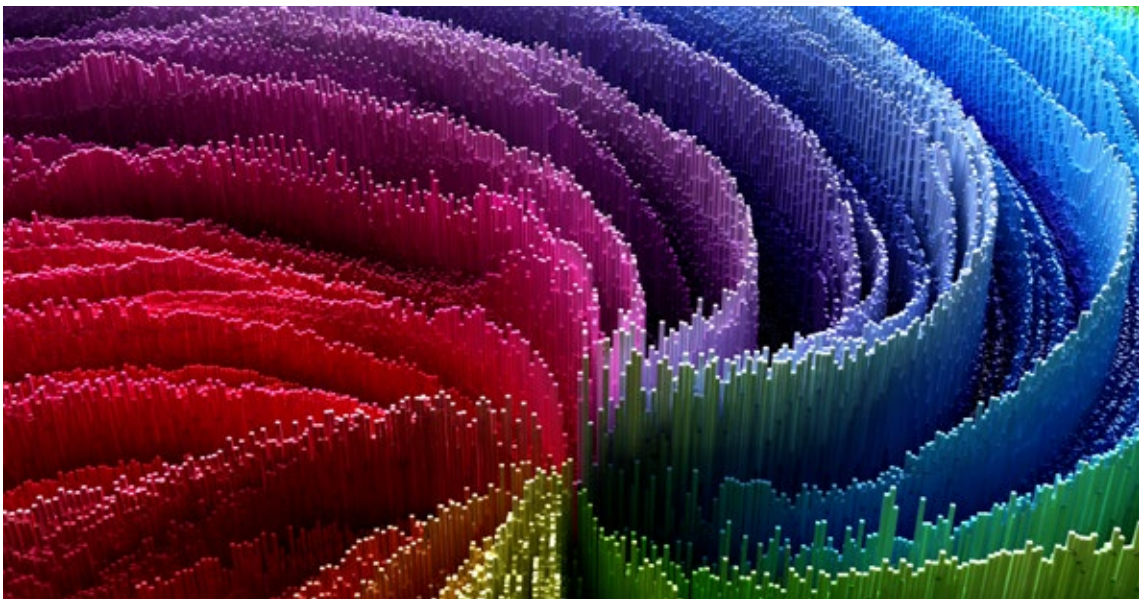
CLEAN DATA

Data is only useful if it is clean, structured and has context. However, often the quality of the health data available is insufficient for many clinical services

– and as one workshop participant observed *"garbage in means garbage out."* In order to gain cleaner data *"we need a common language between all stakeholders."* Several believe that *"the current system does not encourage this. In fact, it incentivises the reverse. As a result, there isn't much communication between specialists, hospitals and GPs."* Furthermore, there is currently very little consistency around how data is collected; notes are written in one surgery which may not be recognized in another thus making it problematic for anyone to manage the transfer of information between doctors. On top of this it is sometimes difficult to ascertain which organisation generated what information in the first place so how to agree who may be reasonably considered responsible for updating and maintaining its quality is almost impossible. This becomes even more complex when you consider that often data is co-created – and then shared. Some see that there has to be a universal agreement to improve standards but at the moment *"even the FDA is struggling to decide what data has to be cleaned."* Moreover, as shown in the graph below, although there has been a rise in the number of doctors using EHRs, those using HER with multifunctional capacity are, in many countries, still low.

CLASSIFIED DATA

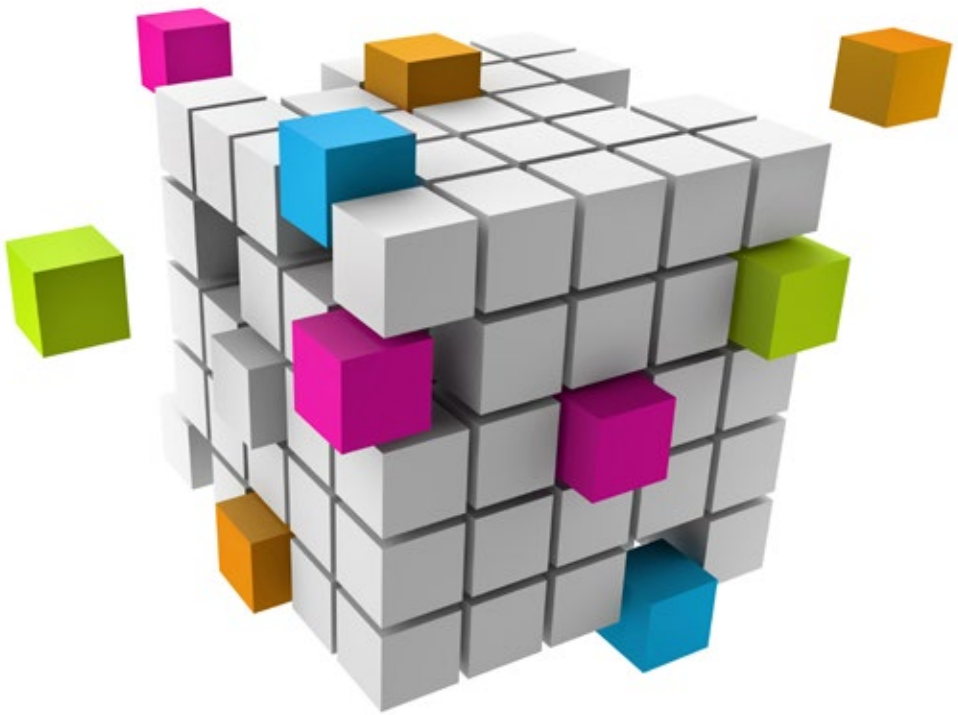
Another important issue is how to manage the combination of high quality medical information with lower quality personal data as well as all the potential proxy data. Present standards around consumer generated data do not meet the higher medical quality thresholds. Many are concerned. *"How do we know what good data is when we are mixing professional information with passive (consumer) data?"* In particular *"Fit-bit data has to have more relevance to make it worthwhile - wearables are not providing medical standard data and so we need to work hard to raise the standards"* and *"there is growing interest in helping consumer generated data to meet medical grade quality levels."*



However, just because data is not of medical quality does not mean it has no value. It's all a question of what information is appropriate. Sometimes *"the data that someone is wearing a fit-bit is itself very valuable and insightful"* – it may be poor quality, but it is a good proxy for healthy activity: *"Who cares about the information quality when we know that someone cares enough about their health to wear a fit-bit?"* Self-reported population data also has great empirical value. *"As long as we know what data we are mixing and can classify it accordingly then we can make good use of the information."* To be useful, some argued, data has to be 'good enough' not always of the highest quality. In San Francisco, the suggestion was that better data classification will provide insight between high value, low value and peripheral information. This reinterprets the challenges to be less about cleaning data and more about how best to combine different quality data sets and use it appropriately: "We have to integrate direct and indirect data." Clearly issues around broader data gaps need to be solved so that it is possible to *"marry up non-traditional data (e.g. weather patterns, air quality, location of parks etc.) with health data"* to better understand patient needs.

INTEROPERABILITY

Many would say that combining datasets has really only ever worked in fairly simple cases with small populations and with relatively few interconnections. With systems as widely varying and disparate as those found across the healthcare sector, it could well be that immense, centralized systems will never completely offer efficient platforms as there are just too many moving parts. Picking the data worth sharing and matching it with the most appropriate platforms around specific issues, conditions, demographics or public vs. private healthcare systems is seen by many as the most pragmatic approach. All the same, most advocate the need for better interoperability, to enable different information technology systems and software applications to communicate, exchange data, and then put the information that has been exchanged to effective use. *"Closing the information loop will foster interoperability and motivate participants to make better use of data."*



THE ROLE OF POLICY

If, as some suggest, we are moving towards universal healthcare data access then we will create a world where information silos are connected, probably via third parties which are able to unify, mine and discover new insights. To do this we will not only have to solve the technological challenge but crack a range of complex ethical and commercial issues as well. Across Europe, despite common ambitions, it was felt that current regulation is preventing progress: *"It's all about interfaces but there is no shared understanding, particularly regionally."* Addressing this is fundamental to the progress of data use within the healthcare system and many felt that *"technically it's not a challenge but policy makers need to step up."*

Beyond political will, some major steps for government-led change include addressing the technological difficulties involved in dealing with centralized and de-centralized interoperability, improving analytics (which varied governments will support to ensure and track standards of care as well as risk stratification) and driving the systems towards better care efficiencies.

It seems clear that as patients and doctors grow more used to new technologies there will be further collaboration across healthcare. *"Getting to an outcome-based system will require a more open market with socially beneficial products utilizing the data aligning with top down government funded activities to build trust."* However, establishing trust in the system will be a long road and not all countries will have the public support nor the technical ability to achieve this for some time. One of the regulatory sticking points, for example, is how to identify an effective way of managing patient consent. Ultimately most believe that necessity will mean that global standards will eventually be created but it will take time; even garnering local agreement in Europe is difficult; America has a different approach; China and India, both of which have more people online than Europe and America have citizens, have another.

AN INTEGRATED SYSTEM

Everyone wants a system where the patient is both active and aware of their involvement in their own care. Several examples of progress, good and bad were cited. In both Oslo and London, the UK care.data approach[27] was mentioned as a failed endeavour – especially concerning the sharing of sensitive medical information with commercial companies without the explicit consent of patients.[28] However the Swiss hybrid model for healthcare[29] was well regarded. Moving forward it is agreed that within Europe there is a lot of positive focus on creating a federation of databases but in doing so we should adopt the FAIR data principles – where Findability, Accessibility, Interoperability and Reusability are all at the core.[30] In the US it is suggested that in order to create the right regulatory environment, it is important to consider *"how to move beyond data harvesting to actually achieving something with the data."*

Within this a number of organisations are seeking to lead change. Companies such as **Validic** (see case study) have already started to combine multiple sources of personal data into one platform that can then be linked to an individual's medical records via the EHR. However meaningfully adding and matching in other proxy data is adding extra complexity. Part of the attraction of organisations such as **Flatiron Health** (see case study) is that they are taking a mass of unstructured data and using expert human input are curating it into a more coherent form for sharing and analysis.

As discussed in more detail later, there are clearly high expectations about the role that varied elements of AI can play in helping with better data integration. However, while some are focused on the longer-term future where the deep learning may better have the capability to deal with unstructured data, for now, many recognise that the first phases of AI application, focused on machine learning and pattern recognition, requires good quality structured data to interrogate. Consequently, there are a wealth of start-ups and new partnerships with the likes of GE, Google, Microsoft and IBM all seeking to help with this data cleaning and structuring.[31]

Perhaps the most notable recent move is however that of **Apple** (see case study) which sees healthcare as a major future area of focus. Given its long-term stance of 'differential privacy' and not extracting value for its customers' encrypted data, the company has now changed its position. In January 2018, after three years of preparing its devices to process medical data, Apple released its updated Health App which has raised the game. Users can now transfer clinical data direct from health providers to their iPhones, sharing the same information with their doctors. The aim is to provide as much transparency and long-terms visibility for personal health information as is available for financial data.[32]

Benefits for the Patient

It is only by having all the varied sources of personal health information effectively joined up that the promise of better use of patient data can be fulfilled. Integration is therefore clearly fundamental to the future ambition. If all of an individual's health records, personal wellness data as well as important proxy data can, indeed, be both co-located and combined, then this is what will open the door to the much-improved analysis, diagnosis and support that all are seeking.

CASE STUDY:

Founded in 2010, US based Validic has become one of the healthcare industry's leading technology platforms for convenient, easy access to digital health data from 'best-in-class' clinical sources. The company has to date raised more than $18 million, much of which came from Kaiser Permanente's venture capital arm. It doesn't monitor patients itself. Rather, it acts as a conduit and dashboard for all the inconsistent data streams emanating from various mobile health and in-home devices, fitness equipment, clinical sensors, activity wearables, smart bands and wellness applications: Information that would otherwise be impossible for doctors and health systems to keep up with and compare.[33] It is providing a one-stop source of much of the non-clinical sources of information that are increasingly part of the patient data mix.

At its core the company is in what it calls the 'conversation economy' which is moving across from social networks into healthcare and helping to provide 'participant-generated data.' "Patients today are expecting more than just episodic care transactions; they're behaving like consumers and want personalized, easy interactions with providers."[34] As such it is focused on improving user engagement through machine learning and seeking to curate a holistic view of wellness.[35] This is important because, as part of the combination, Validic takes data from legacy medical devices that are not even connected to the internet such as a traditional blood pressure cuff. It does this by encouraging patients to take a picture of the reading on their smartphone. For many of the companies that take the output, key issues are simplification, standardization and the means by which to start new conversations with patients. Organisations from hospitals and IT companies to pharma, insurance and health device manufacturers are all customers. So, companies such as Philips integrate the consumer-generated health data from Validic into their own digital platforms that in turn underpin the Philips connected health solutions and services.[36] Moving ahead, the aim is that, as remote monitoring and analytics technologies evolve, the company can provide much more of the increasing portfolio of important health data that is not on the core EHR.[37]

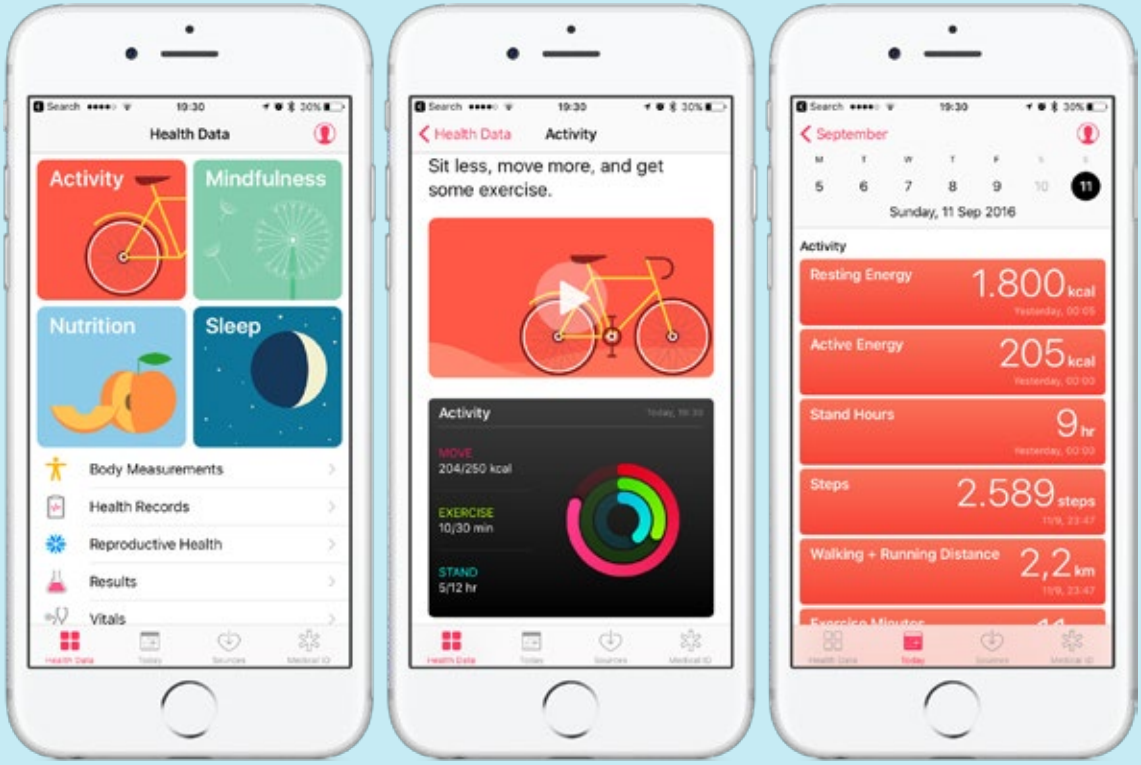
CASE STUDY:

It is little surprise that the world's most valuable tech company has health data ambitions. Although one of the most secretive of the big tech firms, especially concerning long-term aims, some of its digital health ambitions are starting to emerge.[38] After a 'soft-entry' into the market in 2014 with the release of the Health App, the next layer occurred 12 months later with the launch of ResearchKit and the Apple Watch. Since then the company has rapidly built a platform for health data. Apple CEO Tim Cook sees that "health care is big for Apple's future."

Commentators have seen that Apple has several opportunities to exploit.[39] These include:

- Revenues with so much cash that, unlike many others, it is not dependent on insurers' reimbursement.
- Starting with Apple Watch fitness data, an acquisition of Gliimpse[40] (which lets users gather health information from disparate sources and share it with the healthcare institutions) and partnership with Health Gorilla, the company is gaining the clinical-grade data to offer a full personal health record.
- ResearchKit is a platform for large-scale research studies, streamlining the on-boarding process, that has changed the scale at which studies are done and the type of data that can be captured.
- The company has also been involved in diabetes and heart disease-management, connecting patients to the care they need when they need it via partnerships with American Well and others.

In January 2018, after three years of preparing its devices to process medical data, Apple released its updated Health App which has raised the game. Users can now transfer clinical data direct from health providers to their iPhones, sharing the same information with their doctors. The aim is to provide as much transparency and long-terms visibility for personal health information as is available for financial data.[41] The updated Health Records section within the Health app brings together hospitals' and clinics' information to make it easy for consumers to see their available medical data from multiple providers whenever they choose.[42]



However, in a notable departure from its 'we will not see your data' policy due to encryption on the device, Apple now has the caveat for 'users to choose to share it with the company'. For a firm that has previously focused on devices and not data, this signals a potential major shift in future direction. While having the most trusted products through which medical data can flow is still the core priority for growing its core consumer base, the data business is now in play.[43] With the recent recruitment of a wealth of health, biotech and biomedical talent, the ability to embed the next generation of sensors within all its products to generate, capture and analyse more personal health data.

Apple has patents to turn its phones in full medical devices using new sensors to measure blood pressure, body fat and heart function. Equally its headphones are poised to undertake biometric monitoring and the Apple Watch is tracking blood glucose levels and heart health.[44] Furthermore, new apps are coming on line with at least 150 firms globally now developing some form of what have been termed 'digital therapeutics'.[45] At heart, a long-game approach with patients as consumers at the centre seems to fit with Apple's style.[46]

Ownership vs. access

If access to patient data is to have impact it needs to be aggregated and shared but there are concerns around ownership and who makes decisions around its use. Patients may have increasing control of their data, but whether they are its real custodians and are able to control access to it depends on culture, regulation and need. Many countries are moving towards supporting greater individual access and ownership of health data – a question will be how well citizens engage with it.

Everyone is talking about the importance of sharing data but the current ambiguities around how this can be done is proving to be a real barrier. As expectations are growing it is becoming increasingly important to understand who should own health data, who should control it and therefore who should best be able to make decisions around its access and use.

Some believe that ultimate ownership of health records should belong to the individual. After all who else will consider it important to keep that their health records are kept up to date? This is particularly relevant as health data is now being generated on personal devices - pretty much anyone can already take unlimited blood pressures or blood glucose measurements via a smartphone and choose whether or not to share the results.

So why not extend that decision-making ability to other aspects of their health data? But others point out that although organisations and healthcare professionals understand how, where and why to use new sources of data, it doesn't necessarily mean that patients will comprehend what could be the implication of what they choose to share. This might limit their ability to make the right choice about the use of their own records. Also, although the 'informed healthy' and 'worried well' may have good comprehension of what the data is saying, in many regions, concerns were raised about the ability of the 'average patient' or one in acute need or stress to be able to access and control the flow of information necessary for their own care.

REGAINING CONTROL

Although individuals may not fully understand how to control their digital footprints, one thing for sure is that they are increasingly distrustful of some third-party providers that are often in charge of access today. As we become more aware of the way personal data has been used, sold, repackaged and resold, there is a growing swell of public distrust in the current system which allows corporates to hold and capitalize on the use of personal information from the myriad sources they have access to. Not only does this already feel like an unnecessary personal intrusion for some, but many agree that the ways some data is currently stored and shared dramatically increases the risk of privacy breaches. This is either through the deliberate re-selling without permission or unintentionally, because of poor security and the escalation of cyber-attacks. It also raises questions about the need to better regulate the business models - sometimes termed *"surveillance capitalism"* because of their dependence on the sale and resale of personal data. Small surprise, perhaps, why some argue that the only way of regaining control of the situation, certainly for health data, is to ensure that data ownership remains in the hands of the individual who generated it. Whether that is more secure is currently an open question for some. However, looking ahead many believe the patient will not only have access to their own data, but they will increasingly also own it and control it, choosing how it can be shared and with which organisations.

OWNERSHIP

The challenge however is to build consensus around how to achieve this and then how to reasonably manage access data. Currently there seem to be more problems than answers. These were just some questions raised during our workshops:

- Who is responsible and accountable for the creation, upkeep and sharing of associated information?
- Who owns the data today?
- There will be a massive increase in the amount of data, but will ownership also increase?
- All US medical visits are captured electronically, and the data can now be combined – but if this happens who will be in control and manage this?
- How will individuals take ownership?
- What are the costs?
- What about policy impact?
- Once the information is collated, does this actually give individuals improved awareness, and will people better understand their own health risk?

Such is the ambiguity around the issue that there are many approaches around ownership models currently in play even within a single market. For example, in the US the Health Insurance Portability and Accountability Act (HIPAA) does not specify ownership, and state laws are inconsistent. For instance, only New Hampshire has a law which specifically states that patients own their medical records. Legal opinion ranges widely from *"the general understanding of the legal community is that patients own their records, or it's their interests that are ultimately paramount"* to *"the default setting is that the records belong to the provider who has the control over it."* This is in contrast to doctors who, although they are required to store and protect health records, often believe it is the patient who ultimately owns them. *"My understanding is that patients have a legal right to their medical records when they request them. The physician is the caretaker and has the responsibility for maintaining*

those medical records."[47] The situation is much clearer for mental health records as the HIPAA states that these can be only be shared with other providers with the patient's permission.

If that was not complicated enough once data has been aggregated and de-identified the game changes. At this point it can be sold without patient permission. Indeed, the default for many EHR vendors has been that the physician gives them the right to commercialize, de-identified and aggregated data. Currently individuals have no way of tracking this. While HIPPA privacy regulation gives patients the right to review and inspect their personal records, sometimes for a fee, tracing how they are being used once de-identified is pretty much impossible.

CUSTODIANSHIP

Some argue that the current regulation has made the assumption that health organisations should host and therefore control individuals' data. The consequence of this is that in several circumstances patient needs have become secondary to those of the healthcare system. This is why some, especially in Brussels, suggested that the debate should really focus on 'custodianship' identifying who is entrusted with guarding or maintaining health information and how they can be held to account for their actions. This can be considered from a number of different perspectives. For instance, in Western Australia and New South Wales, the Department of Health has a data stewardship policy which puts the focus on custodians managing data on behalf of the state not the patient.[48,49] In Canada, custodians are considered to be individuals or organisations that collect, maintain or use personal health information to provide or assist in the provision of health care or treatment.[50] Here they again have the interest of their employer at the fore but are obliged to respect the wishes of individuals to access or correct their records. Scotland's regional health polices include guidance on providing data to researchers, taking into account the public interest vs individual patient privacy.[51]

TRANSPARENCY

In other countries the situation is no less complicated. But, as understanding grows, so too does concern about how to control data access. To address this one approach is to be more transparent. An early mover here can be found in Denmark where, since 2003, sunhed.dk, an internet-based portal, provides access to medical records for both citizens and health care professionals.[52] Although initially mainly used by GPs, public access has increased substantially in recent years. Some of the big corporates have also tried to improve transparency – but so far with limited success. Microsoft's HealthVault, which launched in 2007 is just one of several opt-in platforms which seeks to enable patients to gather, store, use and share health information.[53] Bringing together medical information from providers and personal data, it expanded from the US to the UK in 2010. Google's version of this, Google Health, closed down in 2012 due to lack of adoption.

Also in the US, one of the most significant initiatives has been Open Notes which now provides over 20m US patients with the ability to review their medical records and report any discrepancies online. In addition, it reminds patients of important next steps, such as diagnostic and screening tests, referrals, and immunizations. Initial evaluations have suggested that this movement may increase patient activation and engagement in important ways and has shown that users have gained greater understanding (of health information), built better relationships (with doctors), received better quality care (adherence and compliance) and improved self-care (patient-centeredness, empowerment).[54]

REGULATION

In Europe, as highlighted in the privacy and security chapter, GDPR regulations are designed to encourage organisations to give back control of personal data to the individual. Although not specific around ownership, these regulations make it easier for individuals to access data which is held on them and to be able to change the permissions they grant

for it to be used or shared. The UK is building on this approach and the NHS now states, *"every citizen will be able to access their full health records at the click of a button, detailing every visit to the GP and hospital, every prescription, test results, and adverse reactions and allergies."*[55] It is clear that, despite its rocky start, the push for transparency marks a significant step towards giving patients more control, and possibly ownership, of their personal information.

It is however India that currently stands out as one of the few nations where the issue is clearly defined. Here the National Health Portal has for some time had guidelines for patient data[56] which state that the *"physical or electronic records, which are generated by the healthcare provider, are held in trust by them on behalf of the patient,"* but that *"the contained data in the record which are the protected health information of the patient is owned by the patient himself / herself."* Patients can not only inspect the information, but also *"have the privileges to restrict access to and disclosure of individually identifiable health information."*

GREATER CONTROL

Whatever the approach, across all our discussions the assumption was that in the future patients will have greater control of their data and be able to access to more information. However, the interpretation of 'control' is varied. Key questions which have yet to be answered concern the benefits of full versus partial control, the link between control and responsibility as well as the improved use of data to give patients a better understanding of their health care choices. In some locations, the debate was around what really constitutes legal ownership – with insurance, pharmaceutical and care provider sectors all suggesting that individuals would not benefit from having sole control of their health data. Others consider that the issue is more about the ability for individuals and organisation to access and use data. *"Patients will have ability to opt-in and opt-out of data sharing and also correct errors."* In other words, it is really all about access vs. ownership?

INDIVIDUAL OVERSIGHT

It is within this area that platforms like **digi.me** (see case study) are now increasingly active. Starting with a pilot in Iceland and now moving to Norway, Australia and the UK, this is enabling citizens to download a copy of all their health data. At its core the aim is to deliver the ambition for individual oversight of all their health data, whatever the source and so put the patient 'in control' of how this is used. In addition, with organisations such as **Nebula Genomics** (see case study) giving the patient the ownership and control of their DNA profiles, the ability for individuals to further control and monetize their health data is moving forward.

In our London discussion, several highlighted the UK Databox research project[57] which focuses on enhancing accountability and giving individuals control over the use of their personal data. This envisions *"an open-source personal networked device or service, that collates, curates, and mediates access to an individual's personal data by verified and audited third party applications and services. It will form the heart of an individual's personal data processing ecosystem, providing a platform for managing secure access to data and enabling authorised third parties to provide the owner with authenticated services, including services that may be accessed while roaming outside the home environment."*

Several organisations who 'can own the patient throughout the whole journey' are confident in their ability to manage access to information through 'joined-up health services' but without having to share data with other companies. Indeed, some felt that *"in 10 years, we will have solved the ambiguity of who owns what."* As *"decision making moves from experts to expert systems"* then maybe the data just becomes an input, or it is transparently monetized and used by all? This may be particularly relevant as *"insurers increasingly need the patient to be part of the system and hit targets (e.g. BMI measures)."* Although some questioned *"if fear of data overload will exceed the individuals' capacity to see things in perspective,"* others put the future focus very much on the capability of healthcare systems as a whole to *"give choice to individual" and so enable the "ability to see and correct your own data."*

Although varied jurisdictions may adopt different approaches and there may be no universal answer, a good number of organisations are already laying the ground for a world in which control of personal data does indeed shift (back) to the individual. The appetite is certainly evident. In Singapore, the view is that *"we will see more democratisation of health information and that is a good thing,"* while in Norway it was proposed that *"patients will become more health literate and so increasingly empowered,"* and hence this will *"drive individual responsibility and accountability that will deliver positive change."*

Benefits for the Patient

Foremost, giving greater visibility on all the health information that exists about an individual is itself a major advance on today. Linking in the ability to then question it and also control it in terms of granting permissions for access to trusted parties takes patient data an important further step forward. While not all may engage, for those that want to, then this shift to custodianship of one's personal data – from across all sources – holds the key for wider empowerment in the years ahead.

CASE STUDY:

Companies such as 23andMe and AncestryDNA charge consumers under $200 to learn about their health or origins; others undertake whole genome sequencing for around $1,000. But all these companies retain control of the data: The customers / patients have no ownership. Co-founded by Harvard DNA sequencing pioneer George Church, MIT start-up Nebula Genomics is seeking to upend this 'exploitation'. It will offer whole genome sequencing, but allow customers to keep custodianship of their data, which they can then rent to the drug companies they choose, potentially making a profit in the process.[58]

Pharma and biotech companies spend billions of dollars each year to acquire genomic data and scientists need large genomic datasets to identify causes of disease and develop cures. However, to date, growth of the genomic data market has been hindered by small data quantities, data fragmentation, lack of data standardization and slow data acquisition. Launched in Feb 2018, Nebula Genomics is leveraging block-chain to eliminate middlemen and empower people to own their personal genomic data. This will effectively lower sequencing costs and enhance data privacy, resulting in growth of genomic data.[59] The company is planning to "spur genomic data growth by significantly reducing the costs of personal genome sequencing, enhancing genomic data protection, enabling buyers to efficiently acquire genomic data, and addressing the challenges of genomic big data. We will accomplish this through decentralization, cryptography, and utilization of the block-chain."[60]

While there are other platforms where people can sell their genetic information online, none offer genome sequencing. Nebula's goal is to get the price of sequencing below $1,000 by working with biotech and pharma companies, which will subsidize a large share of the cost. In addition, people will be able to earn cryptocurrency in exchange for letting pharma companies use their data.[61] People who want to get their genomes sequenced through Nebula will pay with tokens, which will also be used by researchers and companies wanting to acquire that data. Initial modelling proposes that an individual could earn up to 50 times the cost of sequencing their genome – taking into account both what could be made from a lifetime of renting out their genetic data, and reductions in medical bills if the results throw up a potentially preventable disease.

As co-founder and former Google employee Kamal Obbad views it, "under the current system, personal genomics companies effectively own your personal genomics data, and you don't see any benefit at all."[62] Some see the real problem will be whether it is possible to keep the DNA data private while still allowing data buyers to compute on it. With Nebula's model the sequence would belong to the individual, so they could rent it out over and over, including to multiple companies simultaneously. The data buyer would never take ownership or possession of it – rather, it is stored by the individual with Nebula then providing a secure computation platform on which the data buyer could compute on the data. "You stay in control of your data and you can share it securely with who you want to."

CASE STUDY:

UK based digi.me is one of the leading personal data platforms. Operating across a number of sectors including both financial services and healthcare, it allows individuals to connect together multiple data sources.[63] From social media feeds and banking to wearables and health records, it enables users to have a secure personal data library on one of several major cloud-based platforms such as DropBox and Google Drive.

At its core the aim is to deliver the ambition for individual oversight of all their health data, whatever the source and so put the patient 'in control' of how this is used. Linking into personalised healthcare services and treatment its major 2017 pilot has been in Iceland where, as a world-first living lab project, all citizens have universal access to their healthcare data.[64] Iceland is now building on this base to create a broader personal data ecosystem. Other nations are expected to follow suit.

With the advent of GDPR across Europe and US regulation requiring healthcare providers to all create citizen-facing APIs to enable automated data download, the company is expanding quickly. Having merged with its US rival personal.com, digi.me is now working in partnership with a number of EU health systems as well as over 100 healthcare providers in the US via formats including Epic, Cerner and Blue Button. As the global ambition for more patient control of their data, many see digi.me and similar platforms setting the standards.

Trust

In many regions, trust needs to be (re)built between payers, providers and patients as well as with new entrants coming into the healthcare arena. New technology platforms and improving communication with the public both play a major role. Concern about ulterior motives for the use of data is high and some see AI adding to the challenge. Many recognise the need for greater transparency on practice in some pivotal areas.

Trust has traditionally been considered a cornerstone of effective doctor – patient relationships. The need for interpersonal trust relates to the vulnerability associated with being ill, the information asymmetries arising from the specialist nature of medical knowledge, and the uncertainty regarding the competence and intentions of the practitioner on whom the patient is dependent. Without trust patients may well not access services at all, let alone disclose all medically relevant information. Trust is also important at an institutional level, as trust in particular hospitals, insurers and health care systems may affect patient support for and use of services and thus their economic and political viability. Furthermore, without trust it would be almost impossible to carry out effective clinical trials and health research. Another fundamental problem with today's system is that patients lack knowledge and control.

In what has come to be called the post-traditional order the balance of trust is shifting. The days of 'doctor knows best', when patients blindly trusted in and deferred to medical expertise, are being challenged. At the same time breaches in patient data have undermined trust still more. A 2017 survey from Accenture revealed that cyber-attacks have already affected more than one in every four people in the US resulting in an average of $2,500 out-of-pocket costs. Technology has opened the door to vast sources of information and, with various degrees of accuracy, consumers can often self-diagnose, their condition with few choice words and a google search. Today the consumer is 'king' and the 'informed patient' frequently expects to play an active part in decision-making regarding their treatment.[65]

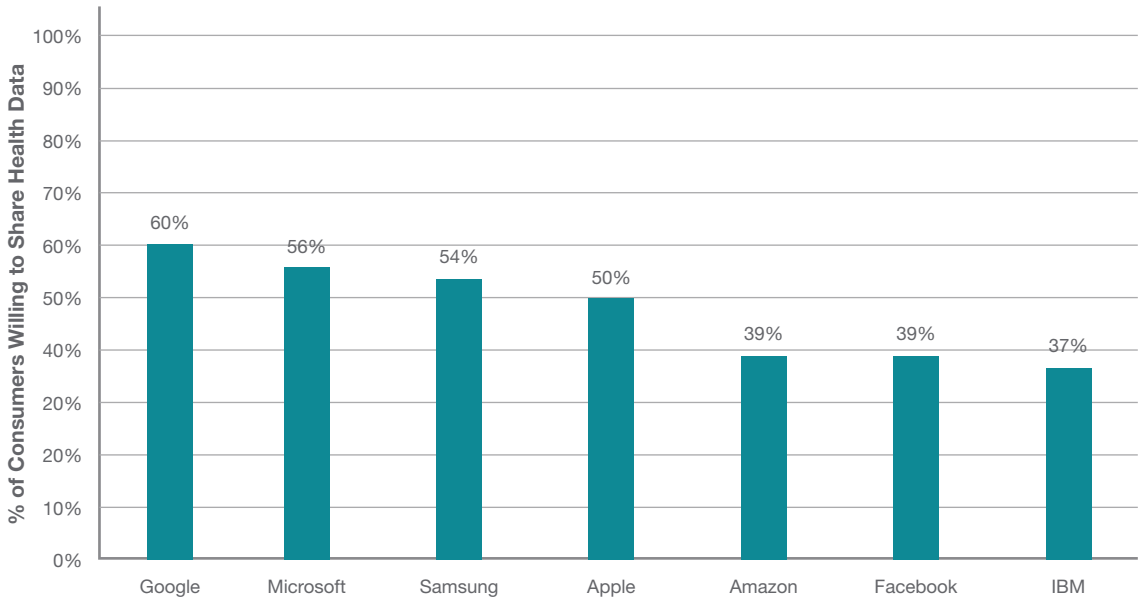
TRUSTED SOURCES

Access to trusted sources of information is therefore essential in supporting consumers as they consider treatment options, shop for health care, and select, buy, and use their health insurance. Yet it seems that many of the trusted sources fall outside the traditional health care system, demonstrating that not just the information but also the information source matters. Looking beyond the immediate patent doctor relationship we are now in a world where, with exception of maybe Canada, the Nordics and Singapore, many regions, public trust in established institutions, especially government, is in deterioration. In South Africa, trust in the national government and the private sector is, for example, pretty low. In several locations we visited, the focus was on how little trust there is between different services – social care, health, aging services etc. and how to use data to build bridges between the different silos.

TRANSPARENCY

We are evidently in a state of flux as, for some, trust has moved away from institutions such as government and the established brands to centre on personal networks. This is having a significant impact on health care delivery. As Eric Topol shared powerfully in his influential 2015 book *'The Patient Will See You Now'* we are entering *"a new era in trust and transparency."*

Consumers Willing To Share Health Data



Source: Rock Health 2016 Consumer Survey

The Edelman trust barometer has for several years highlighted that healthcare as a sector is near the bottom of the rankings alongside financial services. In particular, as trust in pharmaceutical companies continues to slide, *"lesser trust in pharma and biotech companies carries with it broad implications for the ability to attract and keep employees, license to operate in the larger health and business ecosystem, and greater support for regulations that may threaten a license to lead."*[66] Less than half the population trusts healthcare company CEOs and only 70% of employees who work in the healthcare sector say they trust the company for which they work. For healthcare generally, the largest gaps in consumer expectations and how they see healthcare performing lie in the areas of transparency.

As shown in the chart below, very recently there has been good levels of trust in big tech. In 2016, over half of the Americans surveyed in one study said that they were willing to share health data with Google, Microsoft, Samsung or Apple. However, with growing anxiety over such issues as privacy, taxation and fake news, confidence in much of the big tech sector is also falling – just as many are seeking to move deeper into the health sector. This is a big concern for healthcare as many of the new partnerships around better use of patient data are built around collaboration with some of the companies in the spotlight. So, what can be done to address this?

BUILDING TRUST

Implicit within many discussions on how the future of patient data may evolve is the issue of building greater trust. This is not just in terms of personal trust between the patient and the multiple public-facing elements within the health care system, but also regarding the growing cohort of hidden partners that manage, store and utilise patient information. Many agree that *"if patients are to willingly share their data, and if multiple organisations are going to collaborate, there has to be a higher level of public trust than currently exists."*

In Sydney, it was agreed that good regulation is key: *"from a policy perspective, we need to be clear who owns what data and who can share what. We also need to know what information can be accessed in an emergency vs. what data will always requires consent from the individual. This will enable us to agree the right standards and set clear roles."* Broader views on where greater transparency may help to build trust include the pricing and efficacy of drugs. Particular examples highlighted the better use of taxation and how to link funding levels to outcome measures for interventions.

Many believe that one of the most effective ways to build trust is by making information more accessible. *"We need a digital transformation that makes everything easy to use with market and social forces aligning so we can move to better health outcomes based on personalized data."* Many again mentioned Iceland as leading in this space. There citizens are given access to digital copies of all their health data. In London, it was suggested that better communication would do much to build public trust: *"We have to address culture as a barrier to change"* and *"we need to differentiate between real risks and the myths (that are often driven by the media). Key is creating more positive storytelling."* Significantly, *"we need positive early stories to share alongside experiences that matter. There should be clear mutual propositions for sharing and improving transparency."* Beyond this there was agreement that patients should be given greater advice and support so that they can more easily decide what is advisable to share and be given clear choices around whether they should do so – especially on sensitive issues such as sexual or mental health.

BLOCK-CHAIN

Given that one way to establish trust is to increase transparency, several expect that block-chain will have a role to play. The view in South Africa for example was that, despite its limitations, *"we are confident in the security provided by block-chain in terms of it being more difficult to hack but we recognize that it is not as efficient as other options."*

The Canadian government is also investigating block-chain's potential and participants in the Toronto workshop proposed that *"smart contracts may be the best way to utilize it: When more data is liberated then block-chain may have a greater role to play."* But this *"will not impact healthcare 'at scale' in the next 10 years."* Others see that *"using block-chain for health records is a possibility but the idea that this can backdate and work on legacy systems is stretching it too far."* Some consider it to be just more hype and suggest that the noise around this new technology might damage the health debate. *"If we believe trust is an incomplete contract then block-chain is a useful technical tool but doesn't solve the fundamental issue. There are many false expectations and naïve views of block-chain."*

Block-chain has captured the imagination of the healthcare industry, from payers and providers, through pharmacies and product providers. The peer-to-peer network that replaces the traditional role of a centrally trusted authority. More are seeing that leveraging block-chain as a shared bundled-payment platform between providers and payers, greater transparency of price, cost and quality data could be achieved, helping to alleviate the mistrust. In recent Cognizant research, how organisations are planning to use block-chain within healthcare was however notably varied. 44% are planning to adopt a permissioned block-chain that is only accessible to trusted participants while 38% said they are planning to adopt a public block-chain.[67]

Several companies are being proactive about how to use block-chain as part of the mix. Nebula Genomics for one is making interesting moves around allowing patients to own and monetize their DNA profiles. Emin Gün Sirer, co-director of the Initiative for Cryptocurrencies and Smart Contracts at Cornell University has commented that *"the idea of trying to get individuals to monetise their own genomes using the block-chain is an interesting and new one."*[68]

MANAGING DISTRUST

Many are increasingly wary about some of the motivations behind the collection of data. The question raised in Dubai was *"to what extent can we trust organisations who collect and manage our more personalized data and, in particular, our DNA / genomic profiles?"* And then *"how will employers or government use the new health data? Will they select and prioritize treatment and coverage? Is that the natural next stage of health insurance?"* Moreover, "if employers can identify (and recruit) the best and healthiest then what will happen to everyone else? What will happen to those with mental health issues? If the information is available to them, will employers refuse to recruit people who may be prone to depression?" Finally, some ask *"what role can the government play to help manage the problem?"*

In a bespoke workshop with a UK health insurance company, this issue was seen as a major business risk – especially if it raises public concerns which are then fanned by gossip and media speculation. This really is an important issue. As more accurate health data is generated, the possibility that it could be accessed and misused will be impossible to ignore. *"Insurance companies cannot mandate genetic tests, but they may need to differentiate between customers who have them and those who do not."*

In Sydney, the view was that *"no one wants to see a future where genetic profiling means that individuals are excluded from healthcare cover and wider economic or social engagement, such as employment. However, it could happen."* One suggested response was maybe *"insurance companies need to steer clear of using genetic data in any significant way in order to ensure that customers do not feel that they could be penalized."* Traditional risk analysis based on family history and blood tests etc., may well remain the standard point of reference for premium calculation - even though more detailed information is clearly going to be available.

Back in London, this point unpacked wider concerns about the business model for health insurance. Comments included; *"insurance needs to stop looking at data and start sharing"* and *"putting people into smaller and smaller boxes is hugely unhelpful. Some risks are not diversifiable if you shrink the pool*

so that it becomes impractical." Several see that the model for health insurance is currently very primitive and if it is to have relevance in the future then how patient data is used and managed will be critical: *"We assume we are giving our data to someone we trust but organisations (such as Experian for instance) are already gathering it and selling it back to other companies."* With more and better personal information increasingly available over the next decade then a huge 'tsunami of change' may be heading the way of the insurance sector.

THE ROLE OF AI

Many are also concerned about the challenges that AI will uncover – particularly as vulnerable patients might find themselves exploited by increasingly intelligent algorithms. Some are already more comfortable communicating sensitive health issues to electronic devices, machines and chat-bots, rather than humans. What happens if they begin to be manipulated by them? What would happen if an algorithm taught itself a new way to question health data? In the same way that Google Translate AI invented its own language,[69] we risk losing control of our ability to interrogate health data and AI decision-making. The perceptions of trust in how the privacy of NHS patients was treated in the early stages of the partnership with Deep Mind was mentioned several times.[70]

HUMAN TOUCH

Alongside all the technological developments in the mix including wider block-chain use, one company specifically highlighted in Sydney is taking a more human approach to increasing trust in its field of focus. One of the top insights from the 2015 Future Agenda programme was that *"as service provision and consumption becomes ever more digital, automated and algorithmic, those brands that can offer more emotional engagement and human-to-human contact become increasingly attractive."*[71]

In a world of more automation in healthcare, **Flatiron** (see case study) is using a team of humans to sort through patient records and identify the critical data points. Technology cannot yet deal with the unstructured information within which exist the vital signals that point to specific cancer diagnosis, and so the company is using *"human-mediated extraction of data describing human illness, to achieve a level of utility required and explicitly demanded by the human physicians caring for patients, by the human researchers developing new medicines, and by the human regulators evaluating their efforts."*[72] Flatiron has built trust with a very particular community of oncologists and has done it so well that Roche has recently acquired it for over $2bn.

Benefits for the Patient

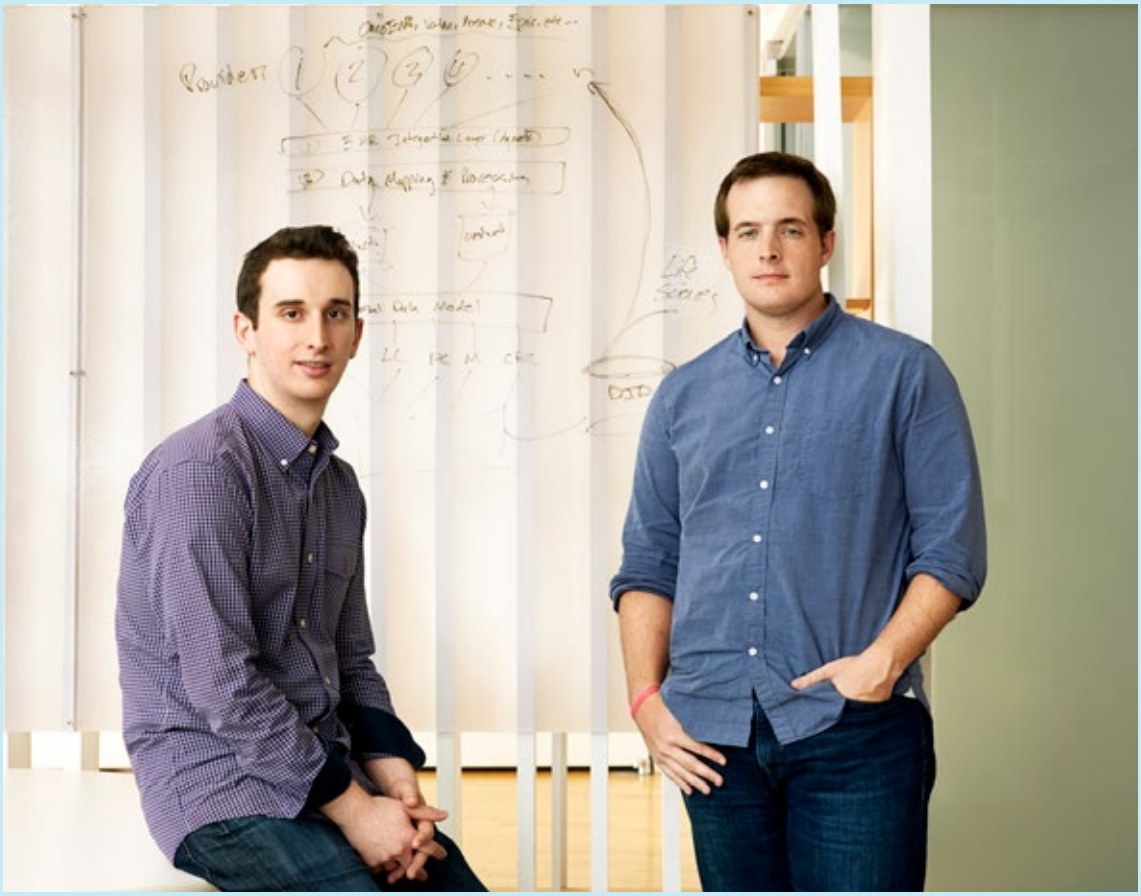
Without trust in the system and healthcare organisations, patients will not be willing to share the all-important data. Whether through better technology or more human touch in the critical moments of truth, building more trust is a primary motivation for many across the sector. Getting this right at a time when trust itself is in such flux is not going to be easy, but it is going to be essential.

CASE STUDY:

An Alphabet-backed start-up, Flatiron has a very different approach to Google. Rather than selling access to users, it provides access to de-identified, aggregated clinical information with a particular focus on cancer. Success is driven by understanding what practicing oncologists really see as meaningful and providing clear value that can help in treating patients. Core to achieving this is a dataset that is distinct in the industry. Flatiron has a "meticulously assembled oncology dataset that pulls information from the electronic health records and organizes it in a fashion that approaches the quality of clinical research, enabling investigators (and regulators) to ask questions of the data that might normally require a dedicated, stand-alone study to resolve."[73]

Given that so much of the available, real-world clinical data is unstructured and stored across thousands of disconnected community clinics, medical centres and hospitals, the core challenge is making sense of all this information. 'In cancer, many of the critical data points reside in documents that are not structured at all. For example, histology. If a cancer is an adenocarcinoma or a squamous cell cancer is something that's in a pathology report, and sometimes it's really distinct, and it's pretty easy to pull that information out. But a lot of the times, it's contextual, and includes a lot of the other information that a pathologist is seeing. And this is not just histology, but information like biomarkers, and what's in the radiology report, and what's in the clinical case notes. 50% or more the critical data points you need for research live in these PDF representations of data."[74]

The company sees that "each patient's story has the unique potential to teach us something new about the way cancer works, and help us find more effective treatments, faster."[75] As such, and given its' heritage, it is notable in its' very human approach. Working with 2m active patients' records, at its core are a sizable team of healthcare professionals who are reading through the unstructured data to extract key insights. While 'technology-enabled' with underlying systems to monitor accuracy and match



information to structured data, the essential work is being done by human beings. Going forward, some expect that AI may deliver efficiency benefits but, for now, the key capability is "human-mediated extraction of data describing human illness, to achieve a level of utility required and explicitly demanded by the human physicians caring for patients, by the human researchers developing new medicines, and by the human regulators evaluating their efforts."[76]

In 2018, Flatiron was acquired by pharma company Roche for a not-insignificant $2.1bn – many expect it to provide access to real world data from a network of oncology practices that can be used to provide a trusted, clinical-research grade record of drug efficacy and utility. This offers the possibility of obtaining regulator-worthy data with unprecedented ease, saving significant money from clinical study costs and delivering the relevant data for quicker decisions - and a faster time-to-market. Flatiron has achieved a level of physician-engineer collaboration that most health tech companies fail to approach and has also strategically partnered closely with regulators, providing FDA with complimentary access to data, and publishing together the results of such analyses. "This helped the company refine the platform, better understanding the questions they should be addressing, while also providing referenceability for pharma companies: if Flatiron data is good enough to be used by the FDA, it's worthy of pharma attention as well."[77] Now with the support of Roche, Flatiron Health is building its capacity to turn health data into insights – "transforming EHR data into analysable, actionable information."

Security and privacy

As anonymized, aggregated data is more easily re-linked and sensitive health data is a target for cyber-attacks, questions are raised around the benefits of centralized vs. decentralized data and the impact of localization. Given both the sensitivity and value of healthcare data it is little surprise that security and privacy are high on multiple agendas. As vulnerability and risk increase apace with greater focus from external hackers and internal sources, these are growing concerns for many.

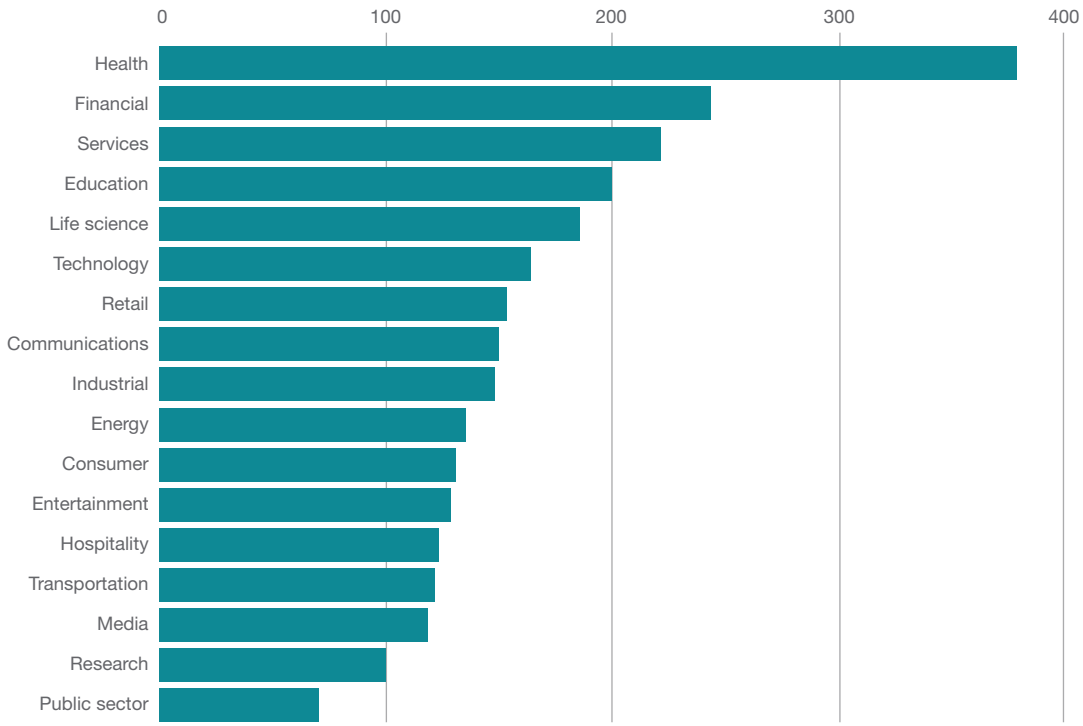
Throughout previous Future Agenda discussions on the future of data and privacy, the vulnerability of health data to hacking has been consistently highlighted. Back in 2010 at a lunch in Washington DC, a prediction was made that *"in the future there will be a 'privacy Chernobyl' that will fundamentally change our attitudes to sharing information."* When pushed to highlight how this may happen, the expert view then was that it would most likely be in US health data as the information has high value, relatively low security (compared to passports and financial services) and lacks agreed standards. Eight years later, a view in San Francisco was that *"Equifax[78] is the canary in the coalmine – and healthcare information is way more valuable than financial information. It is up to 200 x more valuable (especially in a fragmented healthcare system where fraud is possible)."* Today almost a quarter of all data breaches in America happen in health care. In 2015, over 113m Americans' healthcare records were compromised.

THE SECURITY CHALLENGE

Medical data is indeed a popular target for criminals. As highlighted in the graph from FT research below, the average cost per capita of a health data breach in 2017 was calculated to be $380, way more than the $240 for financial data and significantly greater than any other sector. Reuters estimates that medical information is worth 10 times more than credit card information on the black market. Healthcare data can be monetised.

Data Breach Cost Per Capita

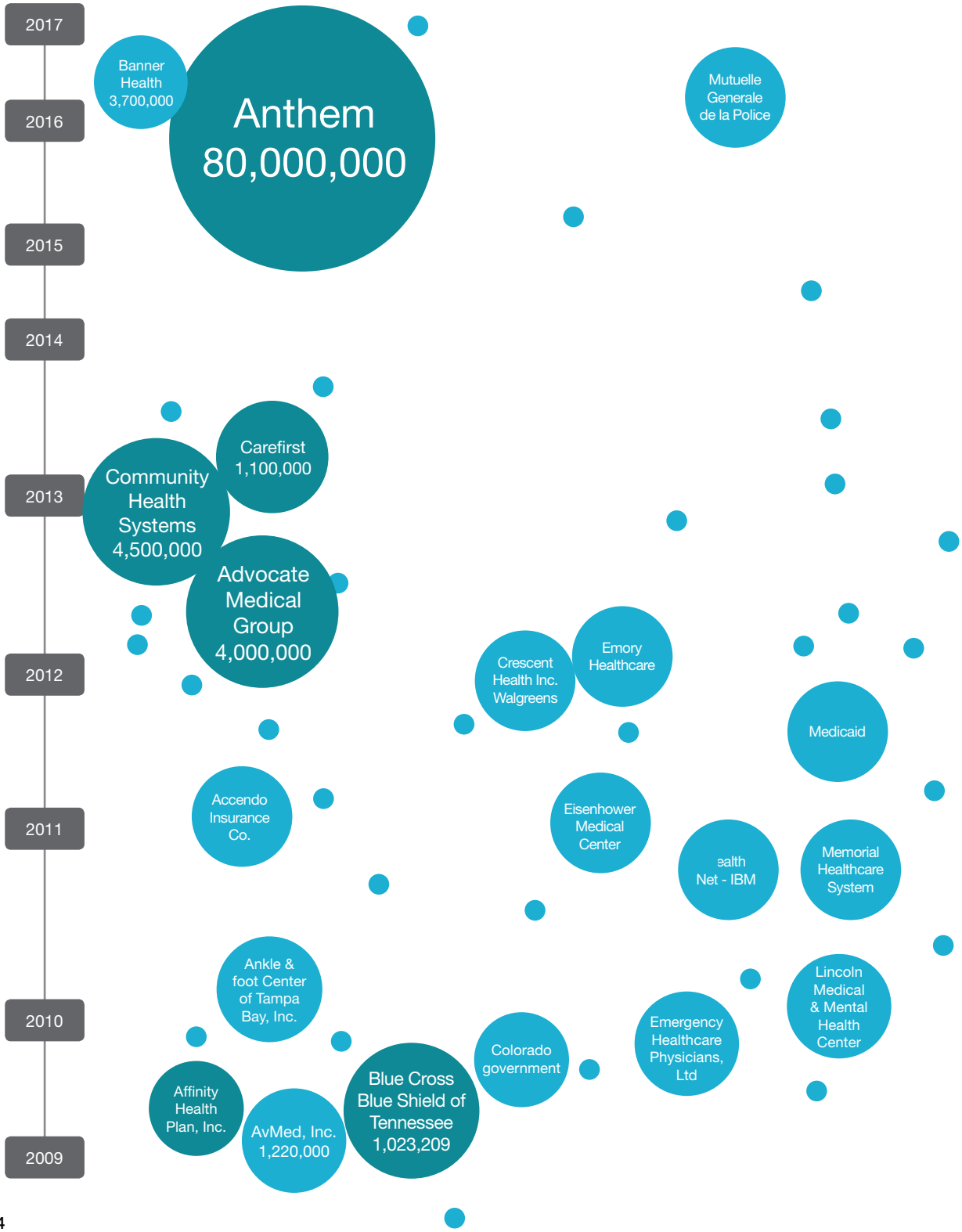
By industry classification, 2017 ($)

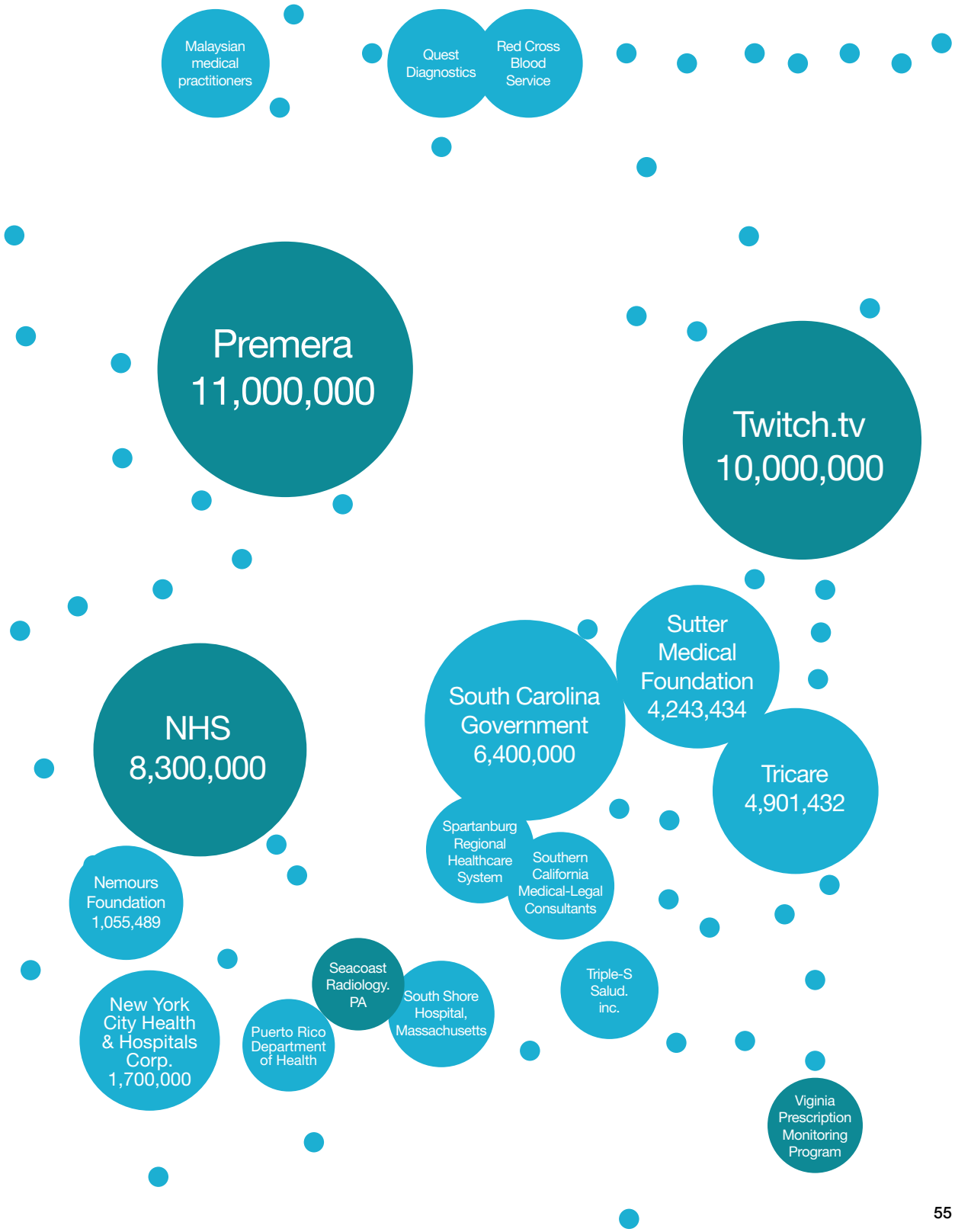


Source: Ponemon Institute / FT

The latest analysis of the world's biggest data breaches (see chart) reveals not only the growing number of attacks but also some of the most significant.[79] Although the 3bn user information Yahoo hack of 2013 is still the largest data hack to date in terms of absolute numbers of accounts compromised, many point to the 2015 breach that gained data on 78.8m customers of Anthem, the second-largest health insurer in the U.S, as having greater financial value.[80] Records accessed included names, dates of birth, social security numbers, addresses, emails and phone numbers. Similar information was gleaned from 4.5m records at Community Health Systems in 2014 and 4m at Advocate Medical Group a year earlier. Although these are also minor in terms of numbers of users when compared to others, given the higher multiples evidently attached to health data, the potential total financial impact of the data loss is far greater.

World's Biggest Data Breaches




Malaysian medical practitioners
Quest Diagnostics
Red Cross Blood Service
Premera 11,000,000
Twitch.tv 10,000,000
NHS 8,300,000
South Carolina Government 6,400,000
Sutter Medical Foundation 4,243,434
Tricare 4,901,432
Spartanburg Regional Healthcare System
Southern California Medical-Legal Consultants
Nemours Foundation 1,055,489
Seacoast Radiology. PA
South Shore Hospital, Massachusetts
Triple-S Salud. inc.
New York City Health & Hospitals Corp. 1,700,000
Puerto Rico Department of Health
Viginia Prescription Monitoring Program

MALWARE

However, while these are significant in terms of value perhaps it was the 2017 infection of a third of the UK's NHS systems as part of the WannaCry malware attack that raised wider concerns on future disruption and data vulnerability.[81] This brought key parts of a national healthcare system to a halt, leading to over 600 cancelled operations and appointments and highlighted that few hospitals had the latest software updates. Ransomware presents an easier and safer way for hackers to gain cash; and, given the potential disruption, most organisations opt to simply pay the ransom. This has unintended consequences of funding more research by attackers who in turn develop more sophisticated and targeted attacks.[82] What is increasingly clear is that the more patient data is stored, shared and analysed in the cloud or shared with different firms, the greater the potential threat of hacking or misuse.

KPMG is just one of many organisations calling for improved security: *"Protecting patients' individual rights, including their personal data needs to be as important as the treatment they receive."* But was is to be done? Cisco, for instance, sees that as well as detecting and preventing malware, securing health and care communities in the future will also require greater cognizance of the vulnerability from the IoT and more connected homes, hospitals and care facilities.[83] Others see that maybe this is more than a traditional security risk.

CYBER-ATTACKS

Beyond financial gain, across all our discussions there was general acknowledgement that health data is increasingly vulnerable to a cyber-attack and there is a pressing need to address the problem. Some are even proposing that health firms should face stringent penalties if they are slapdash about security. The responses to this vary significantly. In Singapore, the view is that there is *"potential future vulnerability to as yet unknown risk from cyber-attacks, coercion or even biological warfare informed by health data and this is why data cannot be shared beyond national boundaries."* Discussions in London and the US noted "focus on bio-warfare and destabilization" and the example mentioned several times (including in follow-on discussions in Bangkok) was the alleged activity of the USAF in mapping Russian genes,[84,85] and the capacity to make weapons that only target one race.

Although many focus on the external threats, most attacks and data breaches in the US system don't come from outside hackers: *"The majority of all inappropriate accesses to EHRs comes from the inside. They involve nurses or doctors, billing specialists, or administrators who have legitimate reasons for having access to systems but who abuse that access for revenge, financial gain or just plain curiosity."* In the US in 2016 there were 450 breaches, affecting 27 million patient records. Of those, 120 incidents were outside hacks, while 200 came from insider actions.[86] Not surprisingly there are many organisations seeking to prevent this or detect it. Protenus is just one of several start-ups focused on tracking behaviours of healthcare workers within hospitals and their access to patient data.[87] It is aiming to improve how healthcare organisations monitor patient data use and does this by using AI analytics to search out anomalous behaviours in health systems. It is effectively automatically policing patient data access and reporting potential breaches.

In its most recent data-breach forecast, Experian predicted that the healthcare sector would be the most heavily targeted industry.[88] It anticipates that "mega breaches will move on from focusing on healthcare insurers to other aspects of healthcare, including hospital networks. These more distributed networks present a ripe target for attackers as it is often harder to maintain security measures as compared to more centralised organisations."

How to store data effectively is another tricky area. *"Patient data appears to be equally vulnerable whether in one centralized database or if it is distributed."* One participant mentioned that *"we*

have 60,000 files on AWS so I am concerned about hacking and breach potential." Although Amazon is one of the more secure cloud services providers, anxiety is there. Finding the right balance to improve security, reduce risk and yet enable the wider sharing of patient data that many desire is going to be a difficult task. Although there is a growing political view in some regions that expresses the right to data privacy and the right to data security the reality is that *"both are illusions: Security is impossible without increased monitoring – and so true privacy is also impossible."*

THE PRIVACY CHALLENGE

In terms of privacy specifically there are mounting challenges and increasingly visibility. Organisations such as the IAPP have been offering advice on the topic for several years.[89] Privacy is now increasingly part of the mainstream conversation and after the recent Facebook / Cambridge Analytica revelations public awareness is rising dramatically. Its implications on healthcare and patient data are also growing. In the UK the NHS and DeepMind came under criticism for the way that the anonymized data of 1.6m patients was shared in 2016.[90]

Around the world, multiple legislative acts are already in place or emerging.

- In the US, health care privacy and security are governed by the Health Insurance Portability and Accountability Act (HIPAA). This limits disclosure of patient data and mandates secure storage and transmission of electronic records. Anybody who violates HIPAA faces civil and criminal penalties. So, the law ensures that providers and health plans take steps to protect your health data and that you retain important rights over how it is used. Similar regulation is in place in a number of locations.
- In force from May 2018 in EU, the GDPR regulation aims primarily to give control back to citizens and residents over their personal data. It sets clear principles that apply to all use of patients' data and to all data controllers.[91]
- In India, the Ministry of Health (MoHFW) has supported a sector-specific law on privacy.[92] Necessitated by the fact that interoperable EHRs are a key component of Digital India, the Healthcare Data Privacy and Security Act will develop a comprehensive legal framework for protection of individual health data and its standardisation and identify the 'ownership' of that data through the establishment of a national e-health authority and health information exchanges.

As highlighted in our project summary map, general privacy regulation is now considered by lawyers to be strong is a wide range of countries including the US, Canada, Western Europe, Australia, Singapore and South Korea and 'robust' in China, Japan, Central Europe and Argentina.[93] Privacy protection specific to health data is now growing in strength in other locations including India, Brazil and much of SE Asia.

ENCRYPTION

Given this, a major challenge is how to balance the level of encryption to preserve privacy while ensuring relevant data is accessible to doctors and so the system is efficient. Today, de-identified data that you share is driving the most important advance in medicine: population-based data discoveries and tools to manage our health, wellness, and diseases.[94] *"There is an illusion of anonymization."* Most agree that the risk of sharing data should be not only recognised, but also made more public. No one is guaranteeing that aggregated or anonymized data can be 100% secure, or that individuals cannot be traced from it, and so, maybe, patients should be made more aware of this? Others agreed that going forward *"no data will be truly anonymous"* and we will see different levels of re-identification. *"Much current health data practice assumes that technology will not be able to be relinked to its source. This is not the case."*

POTENTIAL SOLUTIONS

Addressing the security and privacy challenges while enabling greater patient data access and sharing is plainly a highly problematic balancing act. One proposal is to push anonymization to a greater level – hence the support for the likes of block-chain. Estonia, for instance, is already using block-chain to protect its' citizens medical data. But, while seeming to improve security, this could actually make much medical data more difficult to use for research purposes. A counter-question raised in Oslo was *"as clinical studies data is made more open and put into the public domain, how can we be confident that all will abide by the agreed rules of use?"* In Boston, another view was that the risks from identification of data will be controlled as the *"increasing volume of data being generated makes identification more difficult."* Moreover, *"data is increasingly temporary (e.g. Snapchat) – so the premise of relinking is not true."* Technology will solve the problem so as such the link-ability of open data problem is a *"failed response to managing big data."*

While some of this may be true, others are calling for systemic action.[95] As many healthcare organisations have been slow to adopt practices that have worked for other industries, many do not, for example, use multi-factor authentication. It is standard in financial services but not in healthcare. Going forward healthcare providers should 'apply strong encryption to all patient data and limit who has permission to access medical charts.' An Experian recommendation is that *"healthcare organisations of all sizes and types need to ensure they have proper, up to date security measures in place, including contingency planning for how to respond to a ransomware attack and adequate employee training about the importance of security."*[96] Others point to more bio-metric security as has already being integrated into the Indian Aadhaar system. Whatever approaches are adopted it is clear that if the ambition of wider collection and sharing of patient data is to progress, then a broadening range of security and privacy issues clearly have to be proactively addressed.

Benefits for the Patient

Without security and privacy in the healthcare system, there will be little trust. Without trust patients will not use new platforms nor will they be willing to share more of their personal information with existing healthcare organisations. This is a universal barrier to progress. As individual's digital footprints become more visible, more valuable and more vulnerable to misuse, patients will increasingly expect guarantees from care providers..


network technology <ab2 . net>)
p2p
SECURITY
ork technology <ab2 . net>)
network technology <ab2 . net>)