Chartered Insurance Institute

Standards. Professionalism. Trust.

In association with

SAMI Consulting

robust decisions in uncertain times

# Shaping the Future of Medical Records and Protection Insurance

## Building Trust in Electronic Medical Information Transfer Systems

## About the Chartered Insurance Institute (CII)

The Chartered Insurance Institute is the professional body dedicated to building trust in the insurance and financial planning profession. Our strapline ***Standards. Professionalism. Trust.*** embodies our commitment to driving confidence in the power of professional standards: competence, integrity and care for the customer.

We deliver that commitment through relevant learning, insightful leadership and an engaged membership.

Our 127,000 members commit to high professional standards by maintaining continuous professional development and abiding by our Code of Ethics. The Chartered Insurance Institute is proud to be a member of the Chartered Body Alliance and the Institute for Global Insurance Education


**For further details, contact:**

**Dr Matthew Connell**
Director, Policy and Public Affairs
Chartered Insurance Institute
T: +44(0)20 7397 1125
Email: matthew.connell@cii.co.uk


# Contents

# Foreword by Chartered Insurance Institute

**More information than ever is stored and transmitted electronically. As we check in for flights, file our taxes and switch utility providers electronically, the speed and convenience of electronic data transfer is no longer miraculous, it is simply a hygiene factor.**

As our expectations about the speed and accuracy of data transfer increase, the slow and laborious transfer of paper medical records will become increasingly anachronistic. It will not only cause delays for consumers who are applying for insurance or making a claim, it will increase the risk that crucial information will get missed, that may ultimately deny people cover.

There is no doubt that a strong, effective system of data transfer for medical records will improve outcomes for consumers and help to build trust in insurance.

However, the system must be robust. Medical information is some of the most personal data that can be held about people and the public has to be certain that any system of transferring it is not only secure, but that the intentions of the organisations using it are sound.

This report sets out the steps that need to be taken across the medical and insurance professions, as well as at regulatory level, to create the assurances and safeguards that are needed to build trust.

There is a lot of work to be done, but we must act now to make sure the public gets the secure and efficient service it is entitled to expect.

**Melissa Collett,**
Professional Standards Director
Chartered Insurance Institute



# Executive summary

This independent report looks at the future digitalisation of patient records of people seeking protection insurance. It looks at the current situation, and current problems, the factors that are driving change in the future, and what a good outcome would look like.

**Our underlying assumption is that we are heading towards a situation where digitalisation will be the expected norm. Our report is intended to stimulate debate and action to shape the future of the digitalisation of medical records so that when digitalised records are used for insurance purposes this process happens in an atmosphere of trust between consumers, the medical profession, insurers and financial advice firms and, of course, meets the regulatory requirements of GDPR law and the ICO.**

The Report has been published by the Chartered Insurance Institute and written by SAMI Consulting. It is based on 17 interviews with a wide range of stakeholders across the medical profession, insurance sector and consumer groups to collect evidence and desk research. We also had valuable input from a specially commissioned iPipeline survey of financial advice firms, and legal input from Norton Rose Fulbright LLP. Note the latter input should not be construed as legal advice. The project was supported by a small steering group.

The report finds that there are clear advantages to all stakeholders from using Electronic Health Records (EHRs) – a quicker service for the public and the insurance industry, and a less burdensome one for GPs.

## But EHRs are still only being used in a minority of cases. Why is this?

**Section 1 of the Report examines the current situation and how we got there. There is no single reason for low EHR uptake, but contributory causes include:**

- Historic tensions between representatives of the medical profession and the insurance industry
- Slow uptake of EHR technology by GPs. There are a number of reasons for this including:
  - wider workload pressures on GPs and – in some cases – inadequate IT systems. Information for insurance will never be top of a GP's to do list – and rightly so
  - lack of trust in automated redaction systems intended to filter out the majority of information which is not required for insurance underwriting
  - lack of financial and NHS systems incentives for digitalisation of medical records
- Slow uptake of EHR technology by insurers. The two main reasons are:
  - The "chicken and egg" paradox – low usage by GPs discourages insurance investment and lack of usage by insurers means GPs have to provide information via different processes to different insurers
  - Protection insurers currently seek medical information in only around 20% of cases (for customers who declare significant pre-existing conditions or who seek insurance for large sums). And some insurers focus largely on those customers who are healthy.
  - Lack of awareness of EHRs among Independent Financial Advice Firms – currently IFAs are not engaged in any meaningful way in improving EHR uptake.

# **Executive summary** - continued

## What can drive change?

**Section 2 of the Report identifies the factors that are making it easier to envisage a future based on EHRs as standard practice, including:**

- General public acceptance of digital as the preferred medium for transactions, including confidential ones
- The drive towards integrated and interoperable digital records in the NHS Long Term Plan, along with the Framework for GP Contract Reform, agreed by NHS England and the BMA, which is designed to provide financial and systems incentives to GPs to go digital in terms of patients, the broader NHS and social care sector and non-NHS access to data eg for medico-legal use of subject access requests (SARs), and
- The potential of "big data" as an actuarial and underwriting tool, although this may raise new ethical and possibly regulatory concerns, which the industry is beginning to address.

It also looks beyond the five-year scope of the Report, at how patient records may change in the longer term. Again the GP Contract makes significant promises on patient access to their own medical records.

## What is the legal and regulatory framework and could it change?

**Section 3 of the Report sets out a summary of the legal framework for Data Protection under EU and UK law.**

Under existing law, the GP is the data controller for medical records held by them. Hospitals have their own data controllers for medical records held by them.

The balance between the role of data controller and data processor is a subject of much debate in the IT sector. It is possible to envisage a move to some centralisation of medical records, for example at CCG level. Such a change is considered in the GP contract with CCGs appointing their own data controllers. The legal position of practice responsibility and aggregated data responsibility is also considered in this section.

Overall regulatory responsibility falls to the ICO and for medical data to the National Data Guardian's Office (NDG). The FCA also have also expressed an interest in terms of insurers and banks usage of big data.

## What might the medium to long term future look like?

**Section 4 describes a desirable scenario for five years from now, in which**

- The public's expectations of digital transactions are being met
- EHRs – based on integrated records – are the norm
- Redaction systems are trusted
- There are clear policies and protocols on how the industry uses big data, and
- Agreements are in place between the industry, GP representatives and GDPR regulators on handling and safeguarding of data.

## What should happen to shape a desirable future?

We make five recommendations, which are designed to lay the foundation for this scenario and address today's challenges to moving to a digital future. The first two address the current situation. The second three address the unfolding potential future situation:

**Encouraging EHR use**

We expect that insurance providers and software providers will continue to engage with GP practices to encourage EHR uptake. From this we should see continued gradual progress towards our desirable scenario. But we think two additional actions could help:

- Currently not all protection insurance providers use EHR systems. If the vast majority were to do so this would help to solve the "chicken and egg" paradox mentioned earlier. In addition wider usage of this route by other types of insurers, for example for travel for people with pre-existing conditions, and for medico-legal purposes, for example DWP hearings on works capability assessments would help to build a critical mass of usage
- IFAs are often rooted in their local communities. Most will know their GP surgeries and many may have engagement with them, for example through sales of income protection and liability insurances. From the iPipeline survey we can see they are keen to have a more active role in EHRs. Insurance providers should engage with the IFA community to support their engagement with GP practices on EHR use. And the wider IFA community should exchange experiences of GP practice engagement.

**Recommendation 1:**
The insurance industry should harness IFAs as a new advocate for EHR use, and encourage insurance providers to use EHR as the default route to access to medical records.

# **Executive summary** - continued

**Building trust in EHR systems**

While sterling work has been carried out by organisations such as the BMA and the ABI to set a framework of trust in the EHR process, there is need for more detailed protocols to meet the future digital age for transfer of medical records to insurers and other external users. For the time being this should be based on the assumption that the GP remains the data guardian. A particular sticking point has been the transparency of software redaction systems.

**Data controller roles in the future and the legal framework**

Currently the data controller for medical information is the GP. However the framework for GP contract reform, and the NHS Long Term Plan envisage maximising the usage of NHS data for the benefit of patient care. This is likely to result in some data controller responsibilities at CCG level. It may be that CCGs will wish to take the burden off GPs of processing medical data for external users such as insurers.

**Big data**

Public trust in the use of big data will be dependent on organisations not doing "creepy" things with it. Currently medical data usage for insurance is largely separate from other forms of data held for example though "open banking systems". In the future it is possible to see a blurring of demarcation lines with more data being available on lifestyle preferences that could be used a proxy for health status. A genuine debate is needed to ensure that the future of big data for protection and travel insurance works in the interests of customers

**Patient held data**

It has been promised many times and not delivered, but it looks likely that in the medium to longer term we may actually see patients holding an "e-wallet" of their full medical records. The question arises, what happens if they themselves want to pass relevant medical information from their records to gain access to protection insurance? As with the current situation redaction issues will arise, as will issues relating to confidentiality, resilience of the "wallet", and transfer of data.

There is a prize to be won. For consumers, greater digitalisation could lead to greater trust and claims certainty, because underwriting would be based on medical records and not applicant memory. As for GPs, it could create cost savings and save time responding to life insurance medical report requests.

Although the focus of this study has been protection insurance, the findings and conclusions are potentially relevant to other parts of the industry as well – for example travel, driving and personal injury insurance.

### Recommendation 2:

One obvious solution would be the development of an Article 40 Code of Practice. The Code would be the responsibility of the bodies that draw it up, but the industry should seek to influence the content so that the insurance aspect is reflected fairly and positively.

### Recommendation 3:

GPs' representatives and the National Data Guardian should consider the legal and ethical ramifications of the role of data controllers (currently, General Practitioners) passing on information.

### Recommendation 4:

The IFoA and FCA should consult on what reassurances may need to be given to the public about its stewardship of their personal data; it should keep in view emerging thinking on the impact of big data on actuarial and underwriting standards and ethics and compliance with the Equalities Act 2010, the Data Protection Act 2018, and relevant ethical guidelines.

### Recommendation 5:

The insurance industry should seek to be involved in, or even sponsor, a wide independent debate about how a patient wallet might operate in relation to customer interactions with non-NHS users. If necessary, it should consider the use of external facilitation to help overcome historical disagreements and distrust.

# 1.

# Where we are: and how we got here

# Where we are – and how we got here

**There is a clear consensus among those who run the NHS, the insurance industry, those who regulate data protection, and – most importantly – people who use health services and buy insurance. The future is digital. The shift to digital, which we look at more closely in Section 2 of this report, seems well-set and irreversible, although important technical and ethical concerns cannot be ignored, and there are legal requirements that need to be met, which Section 3 addresses.**

However bright the digital future looks, we need to remember that we are starting from a very low base. Although gradually more reports are being sent by GPs to insurers via Electronic Health Record Systems (EHRs), and most GPs now have access to an EHR system, the proportion of reports sent digitally remains at only about 20%. This reflects low usage by some GP practices and that not all insurers use the EHR process.

**This causes a number of problems.**

- For members of the public, it makes the process of taking out protection insurance longer and slower if medical records have to be obtained manually
- For GPs, manual provision of information is a tedious and time-consuming task, at a time when GPs are feeling overburdened
- For insurers, a manual process is less efficient, and carries attendant risks with regard to redaction of unnecessary information and inadvertent disclosure of information about third parties.

Beyond these headlines, there are other problems. Some GPs have been known to send full print-outs of patient records by standard mail, without encryption or redaction, to insurers. The absence of redaction, which might lead to disclosure of unnecessary personal information, or of information relating to third parties, eg family members, is in clear contravention of data protection law. Insurance companies have indicated that this still happens, and that they tend to deal with it by performing redaction of the data themselves.

## Insurers and the medical profession

It is in everyone's interests to have a system based on EHRs, which is user-friendly and fully complies with data protection laws. There is a history of discussions and negotiations between GPs' representatives (the British Medical Association (BMA) and the Royal College of General Practitioners (RCGP)) and those of the insurance industry. The ABI issued in December 2017 a set of 10 principles for requesting and obtaining medical information electronically from GPs[1]. The principles were drawn up in consultation with the BMA, as well as the Information Commissioner's Office (ICO), which upholds information rights in the public interest, and the General Medical Council (GMC), which is the regulator for the medical profession. They provide a sound framework on which to design and build EHR systems. The principles are as follows:

1. All requests must be made in accordance with an individual's rights under relevant legislation
2. An electronic process must comply with relevant legislation and be reviewed upon fundamental changes to that legislation
3. An electronic process should provide the GP with the ability to redact, amend or add sensitive personal data to an electronic report
4. An electronic process should be clear about what the patient is being asked to provide to the insurer
5. An electronic process must be at least as secure as, or increase the security above, the current system for obtaining medical information
6. An electronic process must provide an audit trail of the consent process and the data sent, making it available to all parties
7. An electronic process should conform to ISO/ BSI Standards or equivalent
8. An electronic process should be compliant with ICO, GMC, and NHS Information Technology guidance and standards and all relevant data transmitted should be encrypted to NHS standards
9. An electronic process should have undertaken a Privacy Impact Assessment or equivalent
10. An electronic process must enable the Data Controller to provide information to a third party in accordance with Data Protection requirements and make clear the onward use of data.

The British Medical Association (BMA) has issued its own guidance to doctors on how to respond to requests.[2]

## Technology today

Software is now available to GPs that not only allows EHRs to be sent, but includes redaction software. This software potentially:

- Allows GP practices to send end-to-end encrypted insurance reports and process insurance reports received on paper
- Could be used by all of the UK life insurance market
- Allows automatic redaction of sensitive and third party information, and
- Can process redacted Subject Access Requests and scanned copies of paper "Lloyd-George" notes.

Our research revealed a widely held view that GPs, as data controllers, cannot leave redaction solely to an automatic processor, but must validate the redaction before sending report back to insurers. However, the presence on the market of an EHR tool that allows redaction to be done electronically – even if subject to validation – ought to be a positive factor in encouraging the use of EHRs. It should speed up the process for GPs, even if they, as data controllers, must still satisfy themselves with the quality of the report and its redaction.

The current situation, where only some 20% of reports are being sent as EHRs indicates that more needs to be done to translate the sound principles and points of agreement, and technological options shown above into everyday practice. There are several reasons for the low proportion of EHRs.

## General Practitioners under pressure

For GPs, responding to requests from insurers is never likely to be near the top of their priorities. And GPs are in shorter supply, at the same time as the population is aging and chronic illness is increasing. A report published in May 2019 by the Nuffield Trust shows that the number of GPs per 100,000 people has fallen from an all-time high of 66.5 in 2009 to 60 in 2018[3].

In order to respond to requests in a way that complies with data protection laws, GPs need to ensure that records have been redacted to ensure that only information relevant to the request is provided, and that there is no disclosure of data relating to any third party – for example a spouse or family member (apart from a family history of an inherited disease which is known to the insurance applicant). This is not a task that the GP can delegate, as it is based to some extent on the GP's own clinical judgment, as well as their legal responsibility as data controller – see Section 3 on the legal framework.

The use of EHRs makes the task quicker and easier, and redaction software should make it easier still. However GPs are not a homogeneous group. Individual practices are to a very large extent self-governing within the terms of their NHS contracts. Individual practices will therefore make their own decisions about how they respond to requests for information, and whether they use EHRs and redaction software.

We have also heard that some GPs' systems lack the processing power to run EHR and redaction software without the risk of the systems "crashing". Clearly this is a concern that goes beyond the question of insurance and EHRs, and affects the prospects of successfully achieving the sort of data integration and interoperability envisaged in the NHS Long Term Plan, which was published at the start of this year.

In summary, it has proved difficult to persuade GPs to use a common platform for the transfer of patient records to insurers. This is in part due to the decentralised provision of GP services nationally, and the lack of an overarching mechanism to bring this about. It is also because, for GPs, EHRs are not their top priority, and they are under other resource and workload pressures. The potential time savings to GPs from using EHRs has not been enough in itself, and we understand that concerns remain, at least among some GPs, about the effectiveness of redaction software.

Clearly it is central to the future successful implementation of EHRs and redaction systems that GPs can be persuaded of the benefits, and reassured about the quality of the software. Equally, it is important to understand why GPs are so reluctant to be persuaded.

Discussions between the insurance industry and national representatives of GPs are important, and have had benefits, for example the 10 principles published in 2017, and listed previously. But it is clear that this avenue of communication needs to be supplemented by other initiatives.

- One obvious solution would be the development of an Article 40 Code of Practice – we say more about this at the end of this section. The Code would be the responsibility of the bodies that draw it up, but the industry should seek to influence the content so that the insurance aspect is reflected fairly and positively.
- We highlight below the results of a survey of Independent Financial Advisers (IFA), which shows a low awareness of EHRs, but enthusiasm for them among those who are aware that they are an option. We also note that some IFAs provide wider insurance advice to GPs regarding their practice and personal insurance needs; they have the potential to become ambassadors for EHRs, and we recommend below that this should be explored.

*1 www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2017/health/requesting-and-obtaining-medical-information-electronically.pdf*
*2 www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/access-to-medical-reports https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/access-to-medical-reports*

*3 inews.co.uk/news/health/gp-numbers-training-doctors-nuffield-trust/*

## Awareness in the Insurance Sector

Reluctance and technical difficulties among GPs may not be the only obstacle to greater uptake of EHRs. There is among insurers, a "chicken and egg paradox" – low usage of EHRs by GPs discourages insurance investment and lack of usage by insurers means GPs are asked to provide information via different processes to different insurers.

## IFAs

As part of this study, we commissioned iPipeline to carry out an online survey of Independent Financial Advice Firms (IFAs). The survey was carried out in May 2019. 160 responses were received. The survey results make interesting reading.

**Awareness of EHRs**

- Only 42.5% were aware that there was an EHR system for collecting medical records electronically, and only 9.5% were aware when it was being used
- Among that small minority, all but one respondent found that using an EHR system meant they received a quicker response than from paper based systems.

**Accessibility**

- 86.5% of all respondents said they would like to use the EHR system themselves to request their clients' medical records. Currently the system operates direct to insurers.

**Organic growth will be dependent on trust**

- 63% agreed or strongly agreed that they were happy to go through an application and answer an insurer's health questions on behalf of a client, with 50% disagreeing or strongly disagreeing that they would prefer fewer medical questions even if that led to more requests for full medical reports from GPs, and 54.5% disagreeing or strongly disagreeing with the proposition that they would prefer to ask no medical questions, with insurers seeking medical record in all cases
- However the majority of those who expressed a view agreed with the latter proposition if it would guarantee a pay out at claims stage
- 70% agreed that if medical records could be obtained very quickly through electronic systems, they would change their answers to the above propositions
- In answer to the question of which they trusted most for security and confidentiality of personal customer data, 56% said electronic systems, and 10% chose paper-based systems, with 35% rating both equally.

**Access to insurance**

- 79% agreed or strongly agreed that more customers would buy protection if access to medical records was faster. 68% agreed that younger people were more frustrated by the slow speed of obtaining medical records
- Finally, a free text question asked "in an ideal world, how would you like medical information from your customers to be obtained. Of 107 who answered the question, 76 replied electronically/digitally/online or similarly.

The survey results suggest that there is low awareness among IFAs of EHRs, but very strong support for EHR systems in principle once people are aware of the option, as well as satisfaction among the minority who have used EHRs. It also highlights concern about the effect of delays on customers, and general acceptance of the security of electronic records and the positive aspects of big data. We return to the implications of big data in Section 2.

**Recommendation 1:**

The insurance industry should harness IFAs as a potential new advocate for EHR use, and encourage insurance providers to use EHR as the default route to access to medical records.

## Lack of trust

As well as the constraints on GPs, and a lack of awareness of EHR as an option, there are issues of trust. Our research and interviews showed several manifestations of this:

- Evidence both from interviews and our desk research that some GPs did not have full confidence in the redaction software currently available, and chose instead to carry out manual redaction, despite the extra time taken; others experienced system difficulties
- A belief that, in spite of the ABI's 10 principles, some insurers or IFAs continue to use SARs as a means of getting patient records
- Concern among some groups about what insurers might do with people's records – in part the issue is entangled with wider concerns about misuse of data by private and third party interests, such as the Care.Data and Google DeepMind cases, but more specifically, research by IpsosMORI in 2016 showed that 59% of the public do not trust insurers, and more granular research by the CII in 2018 showed the major causes of public mistrust to be dual pricing, confidence, protection and speed of claims handling[4].

We are aware that discussions are taking place between the ICO, the BMA and the Royal College of GPs (RCGP) about SARs, including issues of 3rd party disclosure and redaction, and the possible development of a code of conduct under Article 40 of the GDPR. Engagement of the ABI, CII and other relevant bodies, such as the Law Society in this process would potentially help to identify issues of disagreement and resolve them, and to build trust. An Article Code that had the backing of all the parties would help to promote awareness and adoption of best practice, and raise awareness of EHRs as a quicker and potentially better quality option in dealing with insurance requests for medical information.

**Recommendation 2:**

One obvious solution would be the development of an Article 40 Code of Practice. The Code would be the responsibility of the bodies that draw it up, but the industry should seek to influence the content so that the insurance aspect is reflected fairly and positively.

*4 www.insurancebusinessmag.com/uk/news/breaking-news/cii-launches-new-public-trust-index-104881.aspx*

# 2.

# Driving change: what might the future look like

# Driving change – what might the future look like

## A connected country

People in the UK now live in a connected world.  85% of the population has a smartphone[5]; the percentages are 95% in the 16-34 age group, and 91% among people aged 35-54[6]. The UK is second only to Norway in the proportion of people shopping online in Europe. 87% of adults shopped online at least once in 2017, and 48% of people bought groceries online[7]. Perhaps more tellingly, 69% of adults now use online banking regularly[8], an increase from 30% in 2007. People are increasingly accustomed to carrying out transactions online, including highly sensitive business such as personal banking and buying and selling. Younger people are once more the most likely to use online banking, but a survey by SAGA in 2015 found that 60% of over 50s agreed that they liked online banking so much that they "couldn't live without it now"[9].

## The NHS – getting there?

Although the National Health Service (NHS) lags behind the retail and finance sector in its use and promotion of technology, medical records are beginning to reflect this trend: they are becoming digitalised. Patient records can be held in a number of different settings – including the GP surgery with which the patient is registered, hospitals in which they are receiving or have received treatment, and community and mental health services, and social care.

The Government and NHS England have committed the NHS to ensuring that patient records are not only held digitally, but are also interoperable, meaning that it is possible to get an integrated view of the complete patient record. The NHS Long Term Plan, published in January 2019 commits the NHS to

- "protect patients' privacy and give them control over their medical record", and
- "mandate and rigorously enforce technology standards (as described in The Future of Healthcare) to ensure data is interoperable and accessible"[10]

In an ideal world, digitalisation of medical records should create far greater engagement between patients and their medical conditions to improve their prognosis and increase their wellbeing. The NHS has piloted schemes where patients with chronic medical conditions hold their own medical records, and the NHS  Long Term Plan sets out specific proposals to give people with long-term conditions digital access to their medical records by 2020, as well as giving all women digital access to their maternity records by 2023[11].

The evidence of the retail and banking sectors suggests that patients will be very willing to see the implementation of digital access in the NHS. Published research by the Royal College of Physicians shows that people with long-term conditions broadly see patient-held records as helpful to them in managing their health, and beneficial in helping them to negotiate the various agencies they deal with.[12]

## The Topol Report

The Secretary of State for Health and Social Care commissioned The Topol Review: *Preparing the healthcare workforce to deliver the digital future,* as part of the draft health and care Workforce Strategy for England to 2027.

The Topol Review was published in February 2019. It makes recommendations to enable NHS staff to make the most of innovative technologies such as genomics, digital medicine, artificial intelligence and robotics to improve services. These recommendations support the aims of the NHS  Long Term Plan, and the workforce implementation plan, helping to ensure a sustainable NHS.

In particular, the Review advises on:

- how technological and other developments (including genomics, artificial intelligence, digital medicine and robotics) are likely to change the roles and functions of clinical staff in all professions over the next two decades to ensure safer, more productive, more effective and more  personal care for patients
- what the implications of these changes are for the skills required by the professionals filling these roles, identifying professions or sub-specialisms where these may be particularly significant
- the consequences for the selection, curricula, education, training, development and lifelong learning of current and future National Health Service staff.

## Investment and evolution

*"Investment and Evolution: a five year framework for GP contract reform to implement the NHS Long Term Plan"*[13], was published in January 2019 by the BMA and NHS England. It signals the aim of digitalisation of GP services to patients, including digital consultations, digital access to a patient's own records.  More broadly, it sets out financial and systems incentives to GPs to go digital in terms of patients, the broader NHS and social care sector and non-NHS access to data eg for medico-legal use of subject access requests (SARs).

## Enhanced role for clinical commissioning groups?

Currently the data controller for medical information is the GP. However the framework for GP contract reform, and the NHS Long Term Plan envisage maximising the usage of NHS data for the benefit of patient care.  This is likely to result in some data controller responsibilities at Clinical Commissioning Group (CCG) level. It may be that CCGs will wish to take the burden off GPs of processing medical data for external users such as insurers.  While this might expedite the response to requests, it would not be appropriate in cases which called specifically for a medical opinion, as well as information from existing records.

**Recommendation 3:**

GPs' representatives and the National Data Guardian should consider the legal and ethical ramifications of the role of data controllers (currently, General Practitioners) passing on information.

*5 www.consultancy.uk/news/14113/uk-smartphone-penetration-continues-to-rise-to-85-of-adult-population*
*6 www.statista.com/statistics/271851/smartphone-owners-in-the-united-kingdom-uk-by-age/*
*7 www.gurufocus.com/news/492058/uk-online-shopping-and-ecommerce-statistics-for-2017*
*8 www.statista.com/statistics/286273/internet-banking-penetration-in-great-britain/*
*9 www.saga.co.uk/magazine/money/savings/banking/over-50s-online-banking*
*10 www.longtermplan.nhs.uk/publication/nhs-long-term-plan/*
*11 www.longtermplan.nhs.uk/publication/nhs-long-term-plan/*
*12 www.rcplondon.ac.uk/projects/outputs/personal-health-record-phr-user-insights*

*13 www.england.nhs.uk/wp-content/uploads/2019/01/gp-contract-2019.pdf*

## Big data

Beyond the arena of health services, the almost ubiquitous use of smartphones and online transactions means that health data can be collected on apps, wearable tech and voluntarily offered to health service providers and also some insurers – primarily in the PMI sector – although take up is also growing in the protection sector. And health status can to some extent be inferred from broader "lifestyle" indicators, eg gym or sports club membership, and individual spending patterns.

More powerful smartphones, tailored apps, ease of data transmission, artificial intelligence machines, and more powerful computers, with greater data capacity all contribute to the emergence of "big data". There is potentially a wealth of underwriting data available to insurers, to the extent that applicable data protection law permits such data to be used for this purpose.

The question is, how this can be used for the benefit of the customer to provide greater access to insurance and protection products. For example, customers with pre-existing conditions may benefit from a faster application and claims process, as it becomes easier for insurers to establish the facts quickly, without having to wait for weeks, or even months, for medical records.

It is possible to obtain more and better data about individuals. From an underwriting perspective, this allows a potentially more accurate assessment of individual risk, and thus keener pricing of policies for individuals. The iPipeline survey of Independent Financial Advice Firms indicated no great concerns among that group:

- 71% agreed or strongly agreed that more data was good, because the pricing of policies would be more accurate; 73% agreed or strongly agreed that it was good because it would allow people with pre-existing conditions to get cover that would not previously have been available; and 76% agreed or strongly agreed that it was good because it would avoid the need for customers to undergo "memory tests" in insurance applications, and reduce non-disclosure
- Asked about the possible downsides of big data, 54% disagreed or disagreed strongly with the proposition that big data was bad because it made the underwriting process more complex and difficult to explain; 47.5% disagreed or disagreed strongly that it would mean some people losing out, for example having to pay a higher premium – just 18% agreed or strongly agreed; and 43% disagreed or disagreed strongly that big data contravenes the ethical principles of insurance pooling, with only 15% agreeing or strongly agreeing.

On the other hand, we have heard from some interviewees that big data causes some anxiety among some other groups. More accurate assessment of risk may work to the advantage of some, but may work to the disadvantage of others. The Institute and Faculty of Actuaries (IFoA) is currently considering whether to examine the balance that needs to be struck between the more accurate and granular assessment of individual risk that big data is expected to allow, and the desirability of pooling risk to some extent.

The Financial Conduct Authority (FCA) has expressed its concerns about people with pre-existing medical conditions obtaining affordable travel insurance. In doing so it has highlighted both the need for transparency, and the need to ensure compliance with the Equality Act.

This issue goes wider than just protection insurance, and so is not central to this report, but it has been raised by several interviewees, and we have been made aware of the work of IFoA and FCA, and so it is something that ought to be flagged up, as an ethical and policy issue for the industry, and – potentially – a regulatory issue in the future.

It is worth adding that assessments of risk based on big data may prove to be inaccurate in practice, and/or made on false or misleading data. Companies holding large amounts of data may feed public concern about what else they may do with those data. "Don't do creepy things with my data".

**Recommendation 4:**

The IFoA and FCA should consult on what reassurances may need to be given to the public about its stewardship of their personal data; it should keep in view emerging thinking on the impact of big data on actuarial and underwriting standards and ethics and compliance with the Equalities Act 2010, the Data Protection Act 2018, and relevant ethical guidelines.

## Further down the road – what might happen to medical records in the future?

Although this report focuses on the next five years – as a manageable and foreseeable time horizon – it may be worth touching briefly on how medical records and the ownership and management of data may evolve beyond that time.

Firstly, the planned moves to integrated and interoperable patient records imply that there will ultimately be a single health record for every patient. This record may encompass not only records of illnesses and treatment given, including mental health records, but also social circumstances. This would be a logical development from current trends in health care, in which a person's social circumstances are seen as key influencers of their health status, and in which social interventions are seen as equally, if not more valuable in promoting good health and preventing illness, An obvious example – and an important one in an aging population, is the value of physical and mental exercise in the prevention of dementia. Clearly this would raise questions about the legal framework and regulation of such a "big data" approach.

Currently, GPs remain the first point of contact for patients, and as such are the natural keepers of the patient record, and thus the data controllers under GDPR. This may continue: there is continuing public support for, and trust in, the GP system. However, if records are integrated and there is interoperability, it is possible to imagine a centralised (or regionalised) data registry, in the same way as our personal banking records have long since ceased to be the responsibility of the local branch. In such a case, the data controller would, presumably become the agency that was responsible for the maintenance, quality and security of the registry (or registries).

Thirdly, it is highly probable that current initiatives under which patients with chronic conditions hold their own records, and the wider public can obtain access to their records, will – when NHS technology permits – lead to a point when all adults will have online and mobile access to their health records. In many cases this will reduce, and may even remove altogether, the need for insurers to seek information from the NHS – whether it is still the patient's GP, or a records registry elsewhere in the system. If the patient can provide the relevant medical records, then the only need for NHS information, will be when medical advice is required on a matter relevant to the application or the claim.

# 3.

# The legal framework

# The legal framework

## Data protection considerations

The disclosure of patient health records by GPs to insurers is governed by the following regimes, which all apply concurrently:

- the General Data Protection Act 2016 (GDPR)
- the Data Protection Act 2018 (DPA)
- the Access to Medical Records Act 1988 (AMRA) and
- the common law duty of confidentiality, as particularised in guidance issued by the General Medical Council (GMC), which regulates medical doctors entitled "Confidentiality: good practice in handling patient information" (the GMC Guidance).

Oversight and regulation of data protection is the responsibility of the Information Commissioner's Office (ICO). The National Data Guardian's Panel advises on the state of information governance across the health and care system, and works closely with the ICO.

## Summary of the applicable requirements

The decision to disclose information will be made by the "data controller", the entity that, alone or jointly with others, determines the purposes and means of the processing of personal data . This is usually either (1) an individual GP (where the GP is a partner in a general practice) or (2) a GP's employer, where they are employed by a private company, trust or similar.

Identifiable information (ie. personal data) about patients may only be disclosed by the controller for purposes other than care or local clinical audit where the disclosure is subject to one of the following relevant lawful bases for breaching confidentiality:

- the individual has provided explicit consent (there are more detailed rules where relating to children and individuals without capacity to consent) or
- where the individual refuses or withdraws consent, the disclosure is:
  - required or permitted by law
  - permitted by an approved statutory process that sets aside the common law duty of confidentiality or
  - exceptionally, justified in the public interest.

As a general rule, GPs will be required to rely on explicit consent for transfers to insurance companies, as (1) consent is required by AMRA and (2) it is difficult to envisage a situation where one of the alternative grounds listed above applies.

Disclosure is subject to the following additional controls:

- if the disclosure should be made on an anonymised basis, if possible without frustrating the purpose of the processing (if data is fully anonymised, it is no longer personal data);[19] - as a rule, disclosures to insurance companies would not be made on an anonymous basis, as this would frustrate the purpose
- the disclosure must be limited to the minimum amount of information required to meet the purpose. For insurance purposes, this will not usually be the whole record (and disclosure of the whole record is likely to be unlawful on the basis that it is excessive). All non-relevant information should be filtered or redacted from the data set or report. This is known as the "data minimisation principle"[20]
- information relating to living individuals other than the patient should be filtered out or redacted, unless this information is strictly relevant (for example, the fact that the individual's parent suffered from a relevant hereditary disease) in which case, it should be anonymised insofar as is impossible and otherwise subject to the consent of the individual to whom the personal data relates.[21]

An offer must be made to the patient to see a copy of the information or report made about them for insurance purposes, unless:

- the patient has already indicated they do not wish to see it
- disclosure would be likely to cause serious harm to the patient or someone else; or[22]
- disclosure would reveal information about another person who does not consent to its disclosure.[23]

In the event that one or more of the above applies, the remainder of the data set or report should still be made available to the patient[24]. The patient must also be made aware of their right to request amendment of the report to change any point that the individual considers to be incorrect or misleading.

If the doctor refuses to amend the report the individual may attach a document setting out his/her objections to its content; and the discloser must be satisfied that the patient has sufficient information about the scope, purpose and likely consequences of the examination and disclosure, and the fact that relevant information cannot be concealed or withheld.

The patient should be aware (or at least have the option of being aware) of the content of the report, and only strictly relevant information should be disclosed.

## Anonymisation

The GMC Guidance provides that the anonymisation process must be undertaken by:

- a member of the direct care team who has the knowledge, skills and experience to carry out the anonymisation competently, or will be adequately supervised; or
- a data processor under contract with the controller (in which case the data controller maintains responsibility).[25]

Whilst GPs can engage a third party to undertake the anonymisation process on their behalf, they cannot eschew their ultimate responsibility (ie. their duty of care towards the patient) to a third party entity.

## Implications for the future model

Several challenges arise from the current system. Particularly:

- each disclosure request must be managed on a case by case basis by a direct care team that is often resource-challenged. That team has a duty to respond "promptly" and it is generally in the patient's best interests for insurers to make coverage decisions quickly; and
- the data minimisation principle is sometimes breached as a result of entire records being shared without being subject to appropriate filtering, redaction or anonymisation.

Over time it is anticipated storage of patient health records may transition from the current de-centralised model (where the data is held by individual GP practices, whether in a paper format or an electronic format) to a centralised model (with the data being held centrally by an NHS entity).

Given the duty of confidentiality owed by health practitioners to their patients, ultimate responsibility for disclosure decisions relating to patient health records currently sits the direct care team (eg. a GP), even where filtering, redaction and anonymisation are undertaken by a third party. It is unclear whether this will remain the case after transition to a centralised database, but a change in current law would be required to transfer this responsibility.

The data protection position in relation to designing a future model for electronic sharing of patient records with insurers can be summarised as follows:

- the transition from paper records to electronic records does not impact the data protection position
- any transition from a de-centralised to a centralised model will not shift ultimate responsibility for decision making in relation to disclosure of health records (elements of this can be contracted out, but decision making will the controller's risk); and
- transfer of ultimate responsibility from the GPs to a centralised model would require legislative change mandating that the centralised data controller was responsible for making such decisions and exercising the duty of care owed to patients on its own behalf as opposed to on the behalf of the existing controller (ie. the GPs).

*14 Article 4 GDPR*
*15 Paragraph 9 GMC Guidance*
*16 Paragraphs 17-19 GMC Guidance*
*17 Paragraphs 20-21 GMC Guidance*
*18 Paragraphs 22-23 GMC Guidance*

*19 Paragraph 10 GMC Guidance, see also Recital 26 GDPR*
*20 Article 5(1)(c) GDPR, Paragraph 115(c) GMC Guidance*
*21 Article 7(2)(a) AMRA*
*22 Article 7(1) AMRA*
*23 Article 7(2)(a) AMRA*
*24 Article 7(3) AMRA*
*25 Paragraph 85 GMC Guidance, see also provisions relating to processors under the GDPR (and particularly, Article 28)*

# 4.

# A good outcome: what does "good" look like?

# A good outcome – what would "good" look like?

**This section sets out an optimistic picture of the future, based on the widespread adoption of best practice, and conformity with data protection and other ethical considerations. There are good grounds for optimism about the future, but it would be unwise to overlook the possibility that this optimistic scenario cannot be taken for granted.**

There are several factors that could hinder, or even derail progress, including:

- delays and difficulties in delivering integrated records and interoperability in the NHS, despite the best intentions of the Long Term Plan and the Topol Report: the NHS has run into problems with IT transformation programmes in the past, and so the risk of doing so again cannot be ignored
- fragmentation of health services may make interoperability and integration of records more difficult – for example the increasing use of non-NHS service providers such as online GP services
- operational, financial and workforce pressures within the NHS may divert attention away from the work and investment needed to implement the Long Term Plan successfully
- misuse or wrongful disclosure of patient information causing major public and parliamentary concern, which might in turn reduce the appetite for transfers of big data outside the NHS
- difficult relations between the representatives of the medical profession and the insurance industry may obstruct efforts to find workable solutions to the practical and ethical issues involved in rolling out EHRs.

Any or all of the above are possible, and therefore cannot be discounted. However, the consequences for the NHS in particular would be severe. The Long Term Plan is rooted in the understanding that the NHS, faced with an aging population, and thus with an inevitable rise in the numbers of people with chronic multiple conditions (comorbidities) must become more streamlined and efficient, and help people to manage their own comorbidities. For the NHS to "stand still", would therefore, be tantamount to moving backwards.

To a large extent, prevention of these undesirable outcomes depends on the extent to which the NHS is successful in achieving the aims of the Long Term Plan and Topol. But there are two in which the insurance industry has a key part to play:

- ensuring best practice in data security to reassure the public and avoid instances of misuse, and
- improving relations and joint working with the medical profession.

Both are covered in our Recommendations.

For that reason, it is justified that we focus on the optimistic scenario, whilst recognising that the pace of change may not be as rapid as we might hope. It is also true that there is greater public understanding of the value of IT and interoperability today than there was in the late 1990s, when the NHS was formulating its Connecting for Health strategy.

## The optimistic scenario:

### 1. The public expects…

People will become ever more accustomed to carrying out transactions digitally, and will – especially younger people – expect public agencies such as the NHS to be able to allow them to do so. People who work in the NHS – who, when they are not at work, are members of the public as well – will think and expect the same.

### 2. Medical records better and more easily available

Drawing on the previous section, we set out what a good, and realistic scenario would be five years from now. Firstly, the NHS Long Term Plan will be coming to fruition, in terms of interoperability. There will be a unified coding system for recording medical histories.

Patient records will be better integrated, making it easier to obtain an accurate picture of an individual's health and medical history. It will be easy to send records electronically and securely to where they are needed. Some patients – especially those with chronic conditions – will hold their own records, making it even easier for insurers to obtain the medical history information they require to make a rapid and accurate underwriting decision.

GPs will have confidence in redaction software, allowing them to validate reports quickly and confidently. The great majority of medical reports will be sent using EHRs.

### 3. Using big data well

The insurance industry, as well as the NHS will have clear standards and codes of practice in place setting out how it will use and manage "big data" in relation to individuals, and how it will protect and safeguard privacy. It will aim to win and maintain the trust of its customers by doing so. Companies will have their own policies on the balance between more accurate underwriting for individuals, and pooling of risk among a client group.

There will be agreements in place between GPs' representatives and the insurance industry on handling and safeguarding of data, and these will satisfy the requirements of the ICO.

**Recommendation 5:**

The insurance industry should seek to be involved in, or even sponsor, a wide independent debate about how a patient wallet might operate in relation to customer interactions with non-NHS users. If necessary, it should consider the use of external facilitation to help overcome historical disagreements and distrust.

## Next steps

Following publication of this report, we will reconvene and if appropriate reconfigure the working group to consider how best to facilitate taking forward our five recommendations.

We will also seek to continue the debate on our report with interested stakeholders.

# Acknowledgements

The authors would like to thank Munich Re for their support in getting this project off the ground and their valued contribution and continued commitment throughout

This project was sponsored by the following organisations, which were also part of our working group:

- AIG Life
- The Exeter
- Legal & General
- Munich Re
- Royal London
- Zurich.

In addition the working group included:

- CII
- iPipeline
- Norton Rose Fulbright LLP

We are grateful for the information, views and ideas contributed by the large number of people from the sponsors and organisations listed below, who helped us with our research. This sort of project works best when people give their personal views, informed by their knowledge of the context. The opinions expressed should not therefore be regarded as the positions of any of the organisations listed our thanks go to:

- ABI
- Barclays Bank
- Cura Financial Services
- Data Guardian Office
- General Medical Council
- Genomics England
- Guardian Financial Services
- Health Informatics Unit, Royal College of Physicians
- Information Commissioner's Office
- IPSOS Mori
- MedConfidential
- Medical & Dental Defence Unit, Scotland
- Medical Screening Solutions
- Niche Health
- Norton Rose Fulbright, LLP
- Stadn Ltd
- UnderwriteMe



# About the authors

## About the authors

Richard Walsh and David Lye are Fellows of SAMI Consulting (www.samiconsulting.co.uk). SAMI Consulting provides consultancy, research and training in scenario planning – and other futures and foresight techniques – to help organisations develop strategy and policy with an eye on the future.

Richard spent 6 years as Head of Health at the ABI. Before that, he was a senior civil servant responsible for strategic planning at the Department of Health. He has a special interest in the health and protection sector. He is co-Chair of the Building Resilient Households Group and an Executive Member of the Income Protection Task Force he also works on projects for individual private, public sector, and NGO clients.

David has been a Director and Fellow of SAMI Consulting since 2013. Previously he spent 25 years in Government and the Public Sector, including five years as an Executive Director of the former West Midlands Regional Health Authority/Regional Office of the NHS Executive, and fourteen years as a senior civil servant, mostly in the Department of Health. At SAMI he has carried out work for a number of health clients, including the General Medical Council, NHS Providers and the Academy of Medical Sciences.

The Chartered Insurance Institute
42–48 High Road, South Woodford,
London E18 2JP

tel: +44 (0)20 8989 8464

customer.serv@cii.co.uk
cii.co.uk

Chartered Insurance Institute

@CIIGroup



COH_J012606 07/19