Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

[redacted]
The Association of British Insurers
51 Gresham Street
London EC2V 7HQ

14 July 2015

Dear Mr [redacted]

Use of subject access rights to obtain medical records for insurance purposes

As you are aware, the Information Commissioner has been considering the emerging practice of insurance companies obtaining patient medical records through the use of individuals' subject access rights (SARs) under section 7 of the Data Protection Act 1998 (DPA). This issue was brought to his attention, in part, through concerns reported in the media.

The use of subject access requests as a means to obtain medical records for insurance purposes was a matter previously considered by the ICO twelve years ago in correspondence with the Royal College of General Practitioners. At that time we expressed doubts that SARs could be used to obtain medical records for insurance purposes in a manner that would be compliant with the data protection principles. We have taken this opportunity to review our position in light of developments in law, technology, practice and policy.

The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public authorities and data privacy for individuals. In particular it is the duty of the Information Commissioner to promote the following of good practice by data controllers and, in appropriate cases, take enforcement action to ensure compliance. The Information Commissioner, as a regulator with enforcement powers, has the sole discretion on how to use his powers and does so in accordance with his stated regulatory action policy. The information provided by stakeholders has helped inform his understanding of current practices and the perspectives of those concerned with this matter.

A formal assessment of an individual data controller's practices under section 42 DPA has not been undertaken in this instance on the grounds that it is expedient to consider the practice in broader terms than might be possible by focussing on

a specific case involving a specific data controller. We have, of course, reflected upon the materials provided by those organisations with an interest in this issue. This work has helped us understand how subject access rights are being utilised in practice, and will help us when making any assessment in the future.

We have not conducted a public consultation in relation to this matter as we have been seeking to determine, from an appropriately informed position, whether the DPA is being complied with. Whilst we do not publish guidance on the specific practice of insurers using subject access rights to obtain medical records, attention is drawn to the ICO's guidance in The Guide to Data Protection and the Subject Access Code of Practice available to download from our website.

Human rights considerations

As a public authority the ICO is obliged to not act in a way that is incompatible with the European Convention on Human Rights. Given that the DPA is derived from European law, we must be mindful of the rights afforded to citizens under the EU Charter of Fundamental Rights, which includes the right to respect for private and family life, home and communications (Article 7) and the right to the protection of personal data (Article 8).

The nature of medical records

By their very nature medical records contain 'sensitive personal data' as defined by section 2 of the DPA. It should be noted that the information recorded in an individual's medical record may contain sensitive personal data not only about that individual, but also about others.

An individual's medical record may contain extremely personal information that could cause them - or another - harm, distress or anxiety if released. Unless an individual has previously accessed their medical records, or they have the necessary medical knowledge, they may be unlikely to have a meaningful understanding of the nature and extent of the information contained within their records, and therefore the information which may be disclosed to an insurer following the making of a SAR. This point is particularly relevant to the discussion below regarding explicit consent, fairness and giving individuals sufficient fair processing information.

Access to medical reports under AMRA

The law recognises that insurers may have a legitimate interest in confirming medical information about individuals for insurance purposes. The Access to Medical Reports Act 1988 (AMRA) predates the DPA 1998, and although the Data Protection Act 1984 was in force at the time, individuals at that point did not routinely have a legal means to access their own medical records unless they were computerised, and this was not commonplace. Prior to AMRA coming into force it was usual practice for insurers to obtain an individual's written consent to contact their GP and obtain the requisite medical records.

The record of the debate in parliament during the passage of the legislation illustrates the public policy concerns existing at that time. These included a lack of appreciation by individuals about the significance of consent forms being signed and the amount of information contained within medical records, with no guarantee it would not be disseminated more widely. Public health issues were also a feature of the parliamentary debate with the fear being that the patient-doctor relationship could be eroded and that patients may withhold information from their GP as a result if they thought that, at some point in the future, a record of their interaction might later be passed on to a third party and thereby be prejudicial to their interests. Accuracy of records, with a refusal to insure having a lasting impact on the individual, was another issue of concern. It was also felt that there was simply the danger of an unjustified level of intrusion into the private life of an individual through this practice. There was no suggestion that existing data protection SARs provided an appropriate alternative mechanism.

AMRA therefore sets out a statutory regime - with appropriate safeguards - by which medical information about an individual may be obtained by an insurer for insurance purposes. It should be noted that AMRA makes provision for GP reports to be provided to insurers, and is not a regime for obtaining medical records.

We believe that use of subject access rights in the manner described sidesteps the statutory regime under AMRA. Insurers have advised that they do not consider the practice to be unlawful, and that safeguards comparable to those set out in AMRA (or variations having equivalent effect) have, or could be, put into place.

The right of subject access

Section 7 of the DPA confers the right of subject access on an individual. We

explain in the Subject Access Code of Practice that the DPA does not prevent an individual making a subject access request via a third party. Commonly such situations occur in the context of a solicitor-client relationship, which is a fiduciary relationship of trust and confidence where the solicitor's interests are aligned with those of their client.

It is has been suggested that in this instance insurers are similarly acting as an agent of the individual concerned. This is problematic as the insurer's best interests and those of the individual may, in some circumstances, not be aligned and could even be diametrically opposed. Insurers, and their legal representatives, should carefully consider the basis upon which they act on behalf of the individual, and the issues that may arise under the law of agency in this context.

Section 8(3) of the DPA provides that a data controller is not obliged to comply with a subject access request if they have previously complied with a request and a reasonable interval – having regard to the nature of the data, the purpose for which it is processed and the frequency with which it is altered – has not elapsed. This provision allows the data controller to refuse to comply with a SAR where it has already done so within a close period of time. As it currently stands, it is likely that section 8(3) would apply in the case of individuals seeking a quote from a number of insurers, and therefore individuals may be prevented from obtaining the most competitive price for a policy. This could create competition and other regulatory concerns that insurers should consider.

Enforced subject access (s 56)

Section 56 of the DPA creates the offence of "enforced subject access", that is to say it is an offence under certain circumstances to require an individual to produce or supply a copy of a relevant record. A relevant record is one obtained from specified data controllers, using subject access rights, in relation to specified types of record. For the avoidance of doubt, insurers that require the production of medical records by means of exercising subject access rights will not commit an offence of enforced subject access under section 56, as neither the relevant data controllers, nor the records, have been specified at present - though these details are amendable by order.

Avoidance of certain contractual terms (s 57)

Section 57 of the DPA applies to information contained in any health record which has been, or is to be, obtained by the data subject in exercising their subject

access rights. The effect of s 57 is to make any term or condition of a contract void where it *requires* an individual to provide another with their health records.

In our guidance on enforced subject access[1] we consider that the term 'requirement' should be looked at in a wide context. We give the example of an individual not receiving a job if he or she does not make a subject access request:

> "…for instance, it would be considered a requirement if an individual would be left in a detrimental position by not making a subject access request. Similarly, if a request is incentivised, an individual misses out by not making it... …the act of encouraging or incentivising the data subject to use their subject access rights to obtain the information would be sufficient to constitute a requirement."[2]

Insurers, and their legal representatives, should carefully consider the impact of section 57 in light of our guidance in relation to section 56.

First principle – fair, lawful, in accordance with a Schedule 2 and 3 condition

The first data protection principle requires that personal data should be processed fairly, lawfully and in accordance with a Schedule 2 condition and, in the case of sensitive personal data, a Schedule 3 condition in addition.

It is our understanding that the Schedule 2 condition relied upon by insurers in this context is 'consent' and, in terms of Schedule 3, 'explicit consent'. The term 'consent' is not defined in the DPA, but the Data Protection Directive refers to consent as being "specific, informed and freely given". The term "explicit consent" is not defined either, but we explain in our Guide to Data Protection that it denotes a standard in which the individual's consent should be absolutely clear, and should cover the specific processing details, the type of information (or even the specific information), the purposes of the processing and any special aspects that may affect the individual, for example disclosures that may be made.

To meet the condition of explicit consent, we consider that individuals must understand they are allowing their legal right of subject access to be exercised

[1] https://ico.org.uk/media/for-organisations/documents/1042608/enforced-subject-access-s56.pdf
[2] Ibid. para 16-19

on their behalf by the insurer, the implications of this, the type and nature of the information that will be disclosed to the insurer as a result, and how their medical records may be further processed and retained by the insurer. It is our view that, in practice, it will be extremely difficult for an insurer to obtain explicit consent from individuals in this context.

In addition to a condition for processing, we also need to consider the fairness of the processing more generally. Given that full medical records may potentially be disclosed – which, given the nature of a SAR, may include sensitive information having no bearing at all on the insurance being purchased – we think it is unlikely that the processing will be fair in this context for the purposes of the first principle.

Third principle - adequate, relevant and not excessive

The personal data processed must be adequate, relevant and not excessive in relation to the purpose(s) of the processing. An insurer who processes an individual's entire medical record is likely to fall foul of the third principle. We consider that in order to comply with the third principle, data controllers would need to ensure only information actuarially relevant to the insurance product in question is processed.

It has been suggested that irrelevant information has previously been provided to insurers in reports produced under the AMRA regime. Whilst this may be the case, in such circumstances there may be a breach of the DPA by the GP in question. This is not a justification for processing excessive or irrelevant data however, and GPs should ensure they comply with all their legal duties when making any disclosure to an insurer.

We note that insurers have managed to provide policies to individuals until this point without the need to obtain medical records. Whilst we understand that the industry is keen to reduce the number of denied claims, we note the provisions of the Consumer Insurance (Disclosure and Representations) Act 2012 are designed to protect consumers who have taken reasonable care to ensure no misrepresentation is made.

Fifth principle – not kept for longer than necessary.

The fifth principle explains that personal data should only be retained for as long as is necessary for the purpose(s) for which it is being processed. It is a matter for data controllers to determine the appropriate retention period for the data

they hold and to be able to justify this. We take this opportunity to point out that retaining data longer than necessary not only breaches the fifth principle, but also increases risk of data being lost, stolen or inappropriately accessed.

In complying with this principle it is important to be able to justify the continued retention of items of information over time. We have concerns that industry practices may mean that medical record information obtained at the proposal stage is retained, even though the data may have no further relevance in determining eligibility for a product and the premium to be charged. We do not believe there are sufficient grounds for insurers to retain medical records throughout the life of the policy and beyond.

Seventh principle – appropriate technical and organisational measures

The seventh principle requires data controllers to have in place appropriate technical and organisational measures to ensure the security of personal data. We are mindful that the practice may lead to large quantities of sensitive information being stored by insurers, and this increases the risk to individuals should the data be lost or stolen.

We also take this opportunity to remind data controllers there is a real risk that the theft, loss or inadvertent disclosure of medical records may lead to a breach of a kind likely to cause substantial harm or substantial distress to individuals. Such a breach, if it was to occur, may therefore be more likely to result in the Information Commissioner issuing a civil monetary penalty.

Summary

The right of subject access is a key element of the fundamental right to the protection of personal data provided for under Article 8 of the EU Charter of Fundamental Rights which is conferred upon individuals. It is not designed to underpin the commercial processes of the life insurance industry. The Commissioner takes the view that the use of subject access rights to access medical records in this way is an abuse of those rights.

If the specific statutory mechanism provided by legislators for obtaining medical information for insurance purposes is failing to provide the information within the timescales the industry needs, then those affected should seek to review that mechanism and have this subjected to proper parliamentary scrutiny with a view to changing it. Using individuals' own data protection rights to side step the current statutory arrangements designed to meet the insurance industry's needs,

and including important safeguards for individuals, is not the appropriate approach.

If you have any questions regarding this matter please do not hesitate to contact me, or my colleagues Garreth Cameron and Alastair Barter.

Yours sincerely

Jonathan Bamford
Head of Strategic Liaison