A guide to data processing during a pandemic

Olivia Whitcroft, Solicitor and Principal of OBEP, discusses how to set up new health and data-collection practices in a way that also addresses data protection compliance and risks

As I arrived at my children's nursery a few weeks ago, their temperatures were taken, and it was requested that I not come beyond the entrance-way. My husband, who had returned from abroad the week before, was asked to complete a travel questionnaire. This asked him where he had been, whether he had a cough or a temperature, and with whom he may have come into contact. My husband's employer has also cancelled his next work trip, closed its physical offices, and asked all staff to work from home. He was asked to inform his manager if he develops the symptoms of COVID-19. When I tried to sign up for supermarket delivery recently, two supermarkets gave me the option to identify if I was a vulnerable individual who may need a priority slot.

These are examples of measures which many organisations in the UK were sensibly taking — even before government requirements were in place — to seek to limit the spread of the COVID-19 coronavirus, and to protect or assist staff, customers, visitors and vulnerable individuals.

Some organisations are involved with larger-scale data collection and use, including health bodies and researchers who are treating or researching the virus. Technology may also be used to collect and analyse data associated with the virus. For example, NHSX (the digital arm of the UK NHS) has proposed a new app to track with whom users have come into contact, and there are discussions about using location data from individuals' mobile phones to assist in monitoring the spread of the virus.

Data protection should not be a barrier to taking steps which are needed to mitigate significant health risks. Nevertheless, new collection and use of health and other sensitive data creates the potential for significant damage and distress to data subjects. New working environments (such as working from home) also mean data may be accessed and used outside standard office-based data protection procedures.

This article discusses how to set up new health and data-collection practices in a way that also addresses data protection compliance and risks.

Risk assessment

An assessment of data protection risks can be undertaken as part of overall assessments of measures to tackle COVID-19. Consideration of data protection risks need not be complex, but can ensure that new (or changed) procedures and activities, which carry data protection risks, are proportionate to their legitimate (and important) aims.

Where large-scale collection or use of health data is proposed (such as using new technology to collect and analyse large amounts of data), a formal data protection impact assessment ('DPIA') will be required under Article 35 of the General Data Protection Regulation ('GDPR'). A DPIA will also be required if the new activities are otherwise likely to present high risks for individuals, including those which fall within the relevant national regulator's list of high risk processing operations (which, for the UK, is available at www.pdpjournals.com/docs/888042).

Where a DPIA is required, defined steps, including mapping out the information flows, and consulting with data subjects or their representatives, must be included within the risk assessment. Carrying out a risk assessment will enable organisations to identify ways to mitigate the data protection and related privacy risks, without compromising the overall benefits of the new activity.

To give a few examples:

- If your organisation is collecting new health data about individuals, think about how much detail you need for the specified purpose, and who needs to know about it. These should be kept to a minimum, and relevant advice of the government and healthcare authorities should be followed.
- You may need to inform staff or other parties about cases of COVID-19 within your organisation, but it is not usually necessary to name individuals. Consider how you can protect anonymity whilst keeping others safe.
- If your organisation is analysing health or related data for research purposes, consider how and at

(Continued on page 8)

(Continued from page 7)

what stage data can be anonymised or pseudonymised, and how access to source data will be limited.

- If office-based staff are now working from home, assess what measures can be put in place to limit new information security risks. These may include, for example, guidance for staff on home working, or new technology to facilitate secure remote access. This is, of course, relevant to protect all existing personal data, as well as any new data being collected.
- You may have fewer resources than usual to handle data protection matters, such as requests to exercise rights, or even breaches. Relevant staff members may be unable to work, there may be a shift in core roles or activities; or staff may have a reduced ability to access information whilst working from home. Despite these limitations, you can aim to keep individuals informed, and identify ways to prioritise matters based on the potential impact for individuals.

Lawful basis and special category data conditions

A question I am frequently asked is whether consent should be sought for the collection of health data, as a lawful basis (under Article 6 of the GDPR) and special category data condition (Article 9 GDPR). In the context of measures being taken to combat COVID-19, the answer is likely to be 'no' in a lot of cases. Consent must be 'freely given' (Article 4(11) GDPR) and can be withdrawn (Article 7(3) GDPR). If the collection and use of data must go ahead to address the health risks, then giving an option to individuals is not appropriate.

Alternative lawful bases and conditions do, however, need to be identified and documented.

An appropriate lawful basis (Article 6 of the GDPR) may be the following:

Legitimate interests: A lot of organisations may look to apply this basis for activities such as collection of new information about staff or visitors. A legitimate interests assessment is required (which can form part of the risk assessment discussed above), ensuring that the need to collect and use the data is balanced against any risks to the rights of individuals.

Legal obligation: This may apply, for example, if the government or a public health authority requires organisations to collect particular data and potentially to share it with the authority.

Task carried out in the public interest: This must have a basis in law, and is most commonly relied upon by public authorities in the performance of their public tasks. Given the public health issues associated with the virus, it may have wider applicability than other standard activities, though an obvious application may be use of relevant health data by public health bodies.

Vital interests: This basis can be applied if use or sharing of data is needed to protect someone's life, and where one of the other bases is not appropriate. Recital 46 of the GDPR also refers to this legal basis in the context of monitoring epidemics and their spread, so it may have an application for the collection of health data in the context of monitoring the virus.

For processing of health data, an appropriate special category condition under Article 9 of the GDPR, as complemented by the UK Data Protection Act 2018, ('the DPA 2018') may be the following:

Employment law obligations: Article 9(2)(b) of the GDPR covers processing activities which are necessary for employers in order to comply with employment law obligations, including ensuring health, safety and welfare of employees. This may include collection of health information in order to keep employees safe from contracting the virus. In the UK, an 'appropriate policy document' is required. This need not be complex, but should document that this condition is being applied, and the procedures for ensuring other principles are met (such as data minimisation and storage limitation).

Legal claims: Article 9(2)(f) of the GDPR covers processing activities necessary for the establishment, exercise or defence of legal claims. In accordance with guidance from the UK Information Commissioner's Office ('ICO'), this may include collecting health data in order to fulfil duties of care to clients, and to defend against related claims. This condition could be considered, for example, if collecting health data to identify vulnerable individuals who need to be treated differently, or potentially if sharing data about existing cases of coronavirus to protect others (though this should be anonymous information, where possible).

Vital interests: Similar to the vital interests legal basis under Article 6 of the GDPR, Article 9(2)(c) covers processing necessary to protect the vital interests of an individual, where they are physically or legally incapable of giving consent. As above, this may be considered where using or disclosing personal data is necessary to protect someone's life, including in the context of monitoring the virus and its spread.

Public health: The Article 9(2)(i) condition covers processing necessary for reasons of public interest in the area of public health. However, the processing must have a basis in law which provides safeguards for data subjects.

In the UK, section 3 of Schedule 1 to the DPA 2018 provides a basis, which requires the processing to be undertaken by or under the responsibility of a health professional, or by someone who owes a legal duty of confidentiality. Therefore, this would cover, for example, processing undertaken by or on behalf of public health authorities. The variances between the national law and guidance of different EU countries (and the UK) indicates that this Article may currently have a different scope of potential application in the UK to that elsewhere. There is also the option for the EU or individual countries to introduce a new basis in law as a result of COVID-19.

Safeguarding: Article 9(2)(g) of the GPDR (substantial public interest), and paragraph 18 of Schedule 1 to the DPA 2018 covers processing nec-

essary in order to protect an individual from neglect or physical, mental or emotional harm. For the condition to apply, the individual must be aged under 18 or 'at risk' (in other words, has need for care and support), and other conditions must be satisfied, including that the processing is of substantial public interest, and the organisation cannot be reasonably expected to obtain consent of the data subject. As with the employment law condition, an appropriate policy document should be prepared. This condition could be considered, therefore, if there is a need to use information about vulnerable individuals in order to protect them, and where it is not appropriate to obtain their consent.

Explicit consent may be required only where alternative conditions such as these cannot be met. This may be appropriate, for example, for individuals who take part in optional research studies, or who sign up for an optional service.

Organisations should identify in advance what happens next if consent is not given (or is withdrawn), or if they receive an objection to the collection of data (even if relying on an alternative condition). For example, could the proposed activity not go ahead, or is it possible to find an alternative way to facilitate the same end goal?

If it is difficult to identify an appropriate legal basis or special category condition, this may also raise the question of whether the activity is proportionate to its aims. The ICO has advised that data protection will not stop organisations sharing information quickly or adapting to the way they work in the face of COVID-19, but it is about being proportionate.

Transparency and rights of individuals

Individuals should be provided with clear information on why new measures are being taken, and how data will be handled as a result. In many cases, individuals may not have a choice about the data collection and use, so they should be given information about the relevant interests and benefits being pursued.

Individuals must also be told with whom data will be shared, such as if it is necessary to provide information to public health authorities. Retention periods may not yet be clearly defined, but organisations can identify the criteria used to determine retention, and communicate this.

As health data are involved, individuals may also appreciate additional information about the safeguards in place to protect the data and minimise its use.

Individuals will, of course, also have rights in relation to additional data collected, including a right to access the data, a right to object, and a right to request erasure, where appropriate.

Other data protection rules

Other data protection rules must also be addressed, including the following.

Purpose limitation: Ensuring data are only used for the identified purposes relating to the virus.

Data minimisation: Ensuring data are adequate, relevant and limited to what is necessary for those purposes.

Accuracy: Ensuring data are accurate and up to date, and correcting or deleting them if they are inaccurate. This may be particularly important if there is a potentially substantial health impact of using inaccurate data.

Storage limitation: Ensuring data are not retained for longer than is necessary for the identified purposes. As raised in relation to transparency, even if it is not yet possible to define specific retention periods, the criteria and procedures for retention and deletion can be identified.

Information security: Ensuring confidentiality, integrity and availability of data (in all media or locations in which it is accessed and used). Pseudonymisation and anonymisation should be considered. Access to data should be limited to those who need them.

Measures should be in place to identify and address any security breaches, which may have a significant negative impact.

Accountability: Documenting data protection assessments which have been undertaken and measures which are put in place.
International data transfers: Identifying the flows of data, and putting in place additional safeguards for any cross-border data sharing.

Direct marketing

In the UK, the ICO has advised that data protection and electronic communication laws do not stop the government or health professionals from sending public health messages, as they do not count as direct marketing.

Guidance

The ICO has a 'Data protection and coronavirus information hub' at www.pdpjournals.com/docs/888043 containing articles and guidance, which is being updated regularly.

Adapting to change

Risk profiles, and the proportionality of proposed data processing activities, can change over time. The associated compliance issues will change with them. In the case of COVID-19, the period for change may be extremely short. Indeed, as you will know, the risks have changed since I started writing this article: my children's nursery is now closed, and a lot of us are confined to our homes.

Organisations should therefore re-assess the situation regularly, particularly as new information is released by governments, regulators and health authorities. In the short-term, significant changes to data processing activities may be justified, but we can hope that, in the longer term, activities can progress back to normal.

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.uk