Securys

Briefing paper

Enterprise privacy risks in Covid-19 response

Published 2020-05-07

Ben Rapp MA(Oxon) FBCS CITP CISSP-ISSMP CIPP/E CIPM FIP
Principal, Securys Limited

John Lloyd MA(Cantab) CIPP/E
Practice Lead, Securys Limited

Introduction

Large enterprises have large responsibilities – to their staff, to their customers, to their communities. Understandably they want to do their part in the global response to the Covid-19 pandemic, and in many cases the programmes that are being proposed involve the collection and processing of personal data.

While in general the intention behind such programmes is laudable, it's important to remember that health information is treated specially by most privacy regulation around the world because it has such potential for harm as well as good. Disclosing health information to the wrong recipient or misusing it can have serious, long-lasting and in some cases irremediable consequences for the very people you are trying to help.

This feature looks at some of the risks and issues associated with extending corporate data collection to include elements of health information across the three stakeholder groups.

Before getting into the detail, we'll first recap the key principles involved in dealing with this kind of data. Health information falls into the "Special Category" of data under the GDPR, and is subject to similar additional constraints in most privacy regulation globally. This means both that processing is restricted and that the security requirements around processing, transmission and storage are significantly more stringent.

Contents

Lawfulness

Considered from a GDPR perspective there are only three circumstances[1] in which processing of health data by a private sector organisation is permissible:

1. With the explicit consent of the data subject
2. To carry out specific obligations under employment, social security and social protection law
3. As part of a formal occupational health programme under the direction of a medical professional

There have been some recent and unfortunately misguided statements relating to the permissibility of processing "in the public interest". In law, however, this does not apply to private sector organisations unless they have been specifically directed by government in accordance with new or existing legislation. There is no general public interest exception.

It is also important to remember, under the GDPR, that when considering employees in particular consent is rarely available as a lawful basis for processing by the employer. The assumption is that employees are rarely in a position to give free consent to their employer. This creates a tension with other privacy regulations globally, such as the LPPD in Peru or the draft Indian Data Protection Bill, which stress the primary importance of consent even in an employer-employee relationship.

It is not always obvious which regulatory regime applies in the context of multi-disciplinary initiatives being delivered on a global basis; it's important that you look not only at the jurisdiction of planned service delivery but also any other location where processing may be taking place or where you may be considered to be offering services.

As a final point for economically strategic enterprises or large-scale initiatives is that in these unusual times local governments are passing specific legislation or providing other ad-hoc mechanisms to legitimise activities including data processing which might otherwise have been harder to justify. When relying on these kinds of public/private collaboration it's important to remember that any country's scope to legitimise processing doesn't extend past their borders. So for instance a local exemption for a health initiative in an Asian jurisdiction would not remove the need to comply with GDPR if the processing were to be done in an EU country.

> This highlights the key point that when processing health data you cannot apply a single policy globally or assume that GDPR embodies global best practice, and must take account of local legislation and regulatory guidance. Make sure you understand what factors affect the scope of regulation, and therefore which regulators have jurisdiction for each processing purpose.

Transparency and consent

Whether your intention is to process on the basis of consent, or to use another exception, it is particularly important to ensure full transparency when processing health information. This means clearly identifying the proposed processing to data subjects ahead of data collection, and ahead of seeking consent, and being sure that your disclosure includes the purpose of collection, the safeguards you are putting in place for the data, any sharing of the information and the period for which it will be retained. You must also be clear about the data subject's rights, including the right to opt out of processing being done on the basis of consent.

When seeking consent, it must be apparent to the data subject and to the regulator that the consent is separate to any other agreement or existing consent, that it is being freely given – and so there are no possible adverse consequences to the data subject if they withhold or withdraw consent – and that everything has been explained in a manner the data subject is able to understand.

> This is particularly challenging when dealing with a global, multilingual workforce, especially if there are significant variations in levels of education and literacy – as for instance in resource extraction or manufacturing.

[1] We're excluding Article 9.2(e) – processing relates to personal data which are manifestly made public by the data subject – from this analysis as while technically an acceptable exception it's not relevant to this feature.

Specificity of purpose

You must be clear from the outset about the objectives for your data collection and processing. This is particularly important if processing on the basis of consent, since any subsequent extension of procession would require obtaining fresh consent under most global privacy regulation. It's also not possible to compose a compliant privacy notice unless you can be specific about your purposes.

If you choose not to process on the basis of consent – or are unable to, as for instance with employee data under the GDPR – then you also need to ensure that your purpose is clearly connected to the lawful basis, such as legal obligation, that you have chosen.

> A common error is to process on the basis, for instance, of an assumed obligation under employment law without having identified the actual section of legislation that requires the processing. This fails the test of necessity. It's also important to ensure that, if you're relying on a legal obligation, it's relevant to the privacy regulation governing the processing. An obligation under US law does not provide a lawful basis for processing data within the scope of the GDPR – only European or Member State law is applicable.

Minimisation

Health information is subject to particularly stringent constraints around minimisation both of the data collected and the distribution of that data. It is important to ensure that you collect nothing that is not directly necessary for your stated purpose, and that access to the data in identifiable form is restricted only to those who need it.

We see potential issues here in a number of functional areas. Clearly there is a need to ensure that the IT function – which is often both outsourced and offshored – does not have access to the data, even if they support the systems in which it is stored and processed.

We're also concerned about large-scale analytics – for planning or other purposes – using pseudonymised or anonymised data which is too readily re-identified by combining data sources. It is a known issue with both health and location data, both of which feature heavily in Covid response, that they cannot easily be effectively anonymised.

Finally there is a risk of data leakage within HR functions where reasonable uses in capacity management, contact tracing and occupational health give rise to data that could be misused in a wider performance-management context or transferred in unnecessarily identifiable form into planning and governance reporting.

> Continuously and diligently review the need for access to identifiable information across all functions and at a granular level. The information being collected for Covid response is generally both more detailed and more sensitive than would normally have been the case, and the risks of breach and misuse are high.

Security

All information you store and process is subject to security obligations. In the GDPR these are set out in Article 32, which requires you to take particular account of the risks to data subjects that may arise from breach, from loss of or corruption to data, and from misuse, and to put in place appropriate technical and organisational measures to mitigate these risks. The GDPR, unlike some other privacy regulations such as, e.g., the US HIPAA, does not specify any of these measures. However, there is a large body of regulatory advice suggesting that the minimum set of appropriate security measures include both pseudonymisation and encryption of health information at rest and in transit.

In addition, the GDPR specifies that you must have appropriate means in place to assure the effectiveness of the measures you have taken – whether that's internal or external audit, vulnerability scans or penetration tests or any combination of the these controls.

> It's vital that in addition to designing security and privacy in from the outset, including the use of pseudonymisation and encryption, you ensure that you have effective ongoing monitoring of security and compliance, and that you do this without silos. Too often security is seen as an IT responsibility, leaving significant exposures around – for instance – policy compliance and paper processing.

Paperwork

Most privacy regulations require something similar to the GDPR's Privacy Impact Assessment as part of the preparation for any proposed processing that presents significant risks to the data subject – as any processing of health data inevitably will. Under the GDPR you are also required to seek the advice of the regulator before commencing work if you believe that your programme carries a high risk of harm.

It's also important to ensure that there is clarity about relationships both with external service providers and between internal entities. Data sharing agreements, and controller-processor or join-controller agreements must be instituted or updated as part of any Covid response project, and the supporting communications and governance mechanisms must be properly resourced and actually used in practice.

Not only does failure to complete this paperwork expose your organisation to material risk of future regulatory sanction, more importantly these processes were introduced by regulation to serve a real function – making you stop and ask yourself: just because we can, does that mean we should?

> The Privacy Impact Assessment is an important part of the programme feasibility assessment. If used properly, it will highlight programmes whose risk outweighs their potential benefits and those where the costs of implementing adequate security and privacy protection are prohibitive. It's also essential to be clear about controller-processor agreements and practical conduct.

International transfers

We are seeing much of the Covid response from enterprise being delivered by global teams and using global resources, especially technology platforms. In some areas there is also a desire to leverage local expertise globally, for instance by giving access to medical advice. While much of this makes sense from a practical perspective, privacy regulation places a number of constraints on the transfer of information across borders, especially where the information is considered sensitive. Any such international transfer exacerbates our concerns under all of the foregoing headings – transfers must be lawful, transparently notified, necessary and minimised for the purpose, properly documented and subject to appropriate safeguards.

An important consideration, especially when trying to leverage existing resources or stand up new capacity at short notice, is to be sure that the actual data flows are properly understood. When working with new partners, or implementing new infrastructure under time constraints, it is often harder to develop comprehensive data flow maps and understand where data is to be stored and processed.

> Don't allow the urgency of deployment to prevent you from properly understanding the global flow of data in each processing purpose. Make sure that partners and suppliers are transparent about their underlying digital supply chain and that you understand how and where storage and processing capacity is being delivered. Do not compromise on security standards in the interests of speed.

Now let's consider some of the use cases for health information that we've seen arising from the enterprise response to the Covid-19 pandemic:

Employees

Wellbeing and counselling

This very common use case involves extending some kind of text-chat, voice or video-based two-way communication to staff, to allow them to express their concerns and engage with resources provide centrally for advice and counselling.

There is no restriction from a privacy perspective on the provision of outbound advice, naturally. However great care is needed in managing any kind of surveying of staff; not only is any kind of enquiry as to their physical state of health or that of their household clearly processing health information, so is any question about their mood. Mental health is just as much subject to the Special Category constraints, so question around how people are coping with lockdown carry significantly greater regulatory impact than might at first be apparent.

If the responses to such surveys are identifiable, as is usually the case with corporate survey tools, then all of the considerations in this feature are relevant, beginning with the critical questions of purpose and lawfulness. This is a circumstance in which processing can be done on consent provided the survey is clearly flagged as optional and there is no internal identifiable monitoring of response rates that might suggest a negative career impact for those not responding. However, the storage, access control and uses to which the collected information are put must be very carefully controlled.

Note that regulators have given widely varying guidance on such programmes, with for example the Italian supervisory authority indicating that they expect any monitoring of Covid-19 to be the exclusive preserve of the Italian public health authorities, while the UK ICO has guided that employers may undertake information collection of this kind subject to working within the law.

> Most corporate survey tools – for example Microsoft Forms and SurveyMonkey – are not appropriate platforms for Special Category data, lacking both adequate security and sufficient access control. Similarly, many engagement tools including Teams, Hangouts and so forth lack both access control and suitable functions for exercising data subject rights. Make sure your privacy office is consulted before any such outreach programme even enters the design phase.

Screening

Many enterprises are considering a layered screening approach before allowing employees to return to the office or workplace. This generally takes the form of a self-assessment questionnaire to identify anyone who is either symptomatic or exposed to others with symptoms, followed by a remote temperature check on arrival, with a possible diversion to a testing facility if the temperature check is failed.

Absent formal government instruction, such programmes must be justified on the basis of occupational health. If your enterprise does not have a formal occupational health programme with a nominated medical professional who has actual ultimate responsibility, you will need to constitute one before engaging in screening of this kind. It is then vital to ensure that:

1. The process you adopt is the minimum necessary to achieve your objective (assumed to be minimising Covid-19 exposure risk for staff coming in to the workplace). So you should collect no data not necessary for this purpose, and should only collect it from those who are required to, or have chosen to, come in to the workplace in person. Where an employee has the capability to work from home, this should be offered as an alternative to screening.
2. Retention of data must be minimised. There may be some justification for retaining positive results at each stage – both to avoid unnecessary rescreening and to process employee absence – but there is none for retaining negative results. If it is deemed necessary to record that an employee passed screening, this should not include, e.g., retaining a record of their temperature or any other answers or supporting information provided.

3. Access control and data security will be paramount. At each stage in the process the number of people able to identify someone with a presumed positive result should be minimised. This will include physical controls as well as digital ones. Pseudonymisation should be adopted at the earliest possible opportunity and maintained.

> The border between visible concern for staff wellbeing and intrusion into private lives is finely-drawn. Demonstrably minimising data collected and being seen securely to delete data that is no longer relevant are important aspects of maintaining employee trust.

Contact tracing

We are aware of a number of enterprise initiatives aimed at workplace contact tracing in various forms. Technological approaches vary from "traditional" interview-based interventions following positive diagnosis through to in-house and out-sourced phone apps and the use of wearables. In some cases this is building on existing location tracking being used for performance monitoring or workplace safety and access control; in others these are new undertakings.

While the desire – and in some cases the pressing need – to demonstrate effective mechanisms for delivering demonstrable workplace safety is entirely understandable, these initiatives carry considerable privacy risk. It is clear that national government contact tracing programmes face significant privacy headwinds[2] and that there is not yet a single established and accepted technological approach. There are also concerns about the actual effectiveness and accuracy of the available digital contact-tracing mechanisms.

The primary concerns for an employer will be lawfulness, minimisation and security. The former will vary by jurisdiction but it is particularly important that if consent is to be used it can be demonstrated to have been freely given under the standards that apply in the location. We recommend avoiding consent and identifying another appropriate basis where possible. In addition to mitigating concerns over the legitimacy of employee consent, this is particularly important where an existing programme is being extended or there is an intention to use the same technology for other purposes in future, to avoid issues with withdrawal of consent or objections to extension of purpose.

Considering minimisation, there is a clear privacy concern if employee contact tracing or location tracking extends outside the workplace. Unless there is an explicit instruction from or agreement with government it seems evident that any contact tracing programme should restrict its ambit to the workplace – perhaps including employer-provided transportation and any necessary queuing that takes place outside the actual relevant premises. It is also important to ensure that internal access to location or contact information is restricted to the minimum number of users necessary to operate the programme; this is particularly important if the programme is being operated as part of occupational health and so is ultimately under the confidentiality responsibility of a medical professional.

Finally on security there have been a number of incidents – including the notorious case in which the locations of secret defence establishments were revealed by location records from consumer fitness trackers – of location data being breached or misused. Particularly where existing consumer location tracking devices, such as wearables, are being used, or when bespoke apps are being developed at speed there is a heightened risk of breach – either through errors in application design or because of in-built features of the underlying platform meaning that location data is automatically also sent to the device or operating system manufacturer. This can be mitigated by using alternatives to location tracking, such as Bluetooth beacons, but these have other associated practicality and security risks.

> If an employer-operated contact tracing programme is considered necessary, or is mandated locally, then great care must be taken to maintain security and minimisation. It will also be vital to ensure adequate transparency as monitoring of this kind will naturally present a material privacy concern to employees, especially once the immediacy of the pandemic has receded.

[2] See also: https://www.linkedin.com/posts/benrapp_privacy-implications-of-contact-tracing-apps-activity-6655724094945849344-xYyR

Telemedicine

A further extension to corporate engagement with employee health has been the rise in telemedicine consultations being offered as an employee benefit to substitute for reduced availability of normal GP services – or for employees in locations where such services aren't readily available even in normal circumstances.

The issue here is not the provision of the service itself, it is firstly ensuring that the telemedicine provider – normally an outsourced service – provides appropriate privacy notifications to staff, including proper coverage of international data transfers where the telemedicine provider or their subcontracted doctors are not in the same jurisdiction as the employee, and controlling sharing of information between the telemedicine service and the employer.

Telemedicine provision is also likely to give rise to complex controller-processor relationships, especially where internal medical resources may be being used alongside outsourced or contract provision via a third-party digital health channel.

While it might seem natural for the service to provide usage information including identifiable data, this should not in fact be the normal position unless there is a local requirement to account for use of the service as a taxable benefit on a per-use basis. Otherwise there is a danger of further analysis of usage patterns or intensity leading to effective processing of sensitive employee data by the employer rather than the telemedicine provider.

> When using third-party service providers for data processing it is essential to ensure that proper due diligence is performed and that employees receive comprehensive disclosure of privacy information. In general we would expect a telemedicine provider to be in an individual controller arrangement with the employer, such that the employer does not have access to or influence over the collection and processing of data by the telemedicine provider; there may be a need for a limited joint controller arrangement for sharing information for billing and tax purposes.

Testing services

Some large enterprises, especially in areas where governments are unable to provide Covid-19 testing in sufficient volume or with acceptable response times, have begun developing testing capabilities internally or in conjunction with service delivery partners. These testing services may be used in a number of ways: initially as the follow-up to screening, then extending into either random or ubiquitous employee testing and finally in some circumstances offered more broadly as a public service or to dependents of employees. We consider these last two cases later in this feature.

Plainly any such programme, when considering employees, must be part of an occupational health programme as noted earlier under screening. However, further consideration is needed regarding obligations of confidentiality, especially when considering the possible consequences for the employee and their contact circle of a positive diagnosis.

> Given concerns about the sensitivity of Covid-19 diagnosis, and the likelihood that programmes of this kind are more likely to be implemented in areas without effective public health programmes, particular attention should be paid to for instance assuring sample pseudonymisation and minimising the risk of diagnosis propagating back up the screening chain. Only the employee and the responsible physician in the occupational health programme should have access to the identifiable diagnosis unless local government instruction requires other reporting.

Customers

Wellbeing and outreach

It's very tempting for marketing and customer service alike to show their concern for customer well-being in these trying times. While the intention may be well-meaning, there can be serious privacy risks inherent in the execution. We're seeing two that concern us:

"Covid-19 Service Update" emails, often presented as a message from the CEO. The general body of these emails is often a combination of uplifting message and genuine information about the business's service readiness.

However, the closing paragraphs almost always contain either an explicit marketing message or a more general exhortation to, for example, "watch out for new availability of product *x* announced on our website". These are marketing messages, and as a consequence make the whole email a marketing communication. Unless you can evidence that you have prior consent from the recipient to receive marketing communication by email, that makes it a breach of the ePrivacy directive within the GDPR scope, and of other regulations such as CAN-SPAM elsewhere. Regulators have been relatively active in enforcing regulations around marcomms, and it's unlikely that they will relax their position because of the pandemic.

> Resist the temptation to use the pandemic as an excuse to send marcomms to opted-out recipients, or to combine genuine service information to active customers with brand-build to a wider audience. The potential fines are significant, as is customer resentment.

The other area of concern, which has considerably greater impact, has been a tendency to include Covid-19 physical or mental health questions in customer outreach surveys. Although, conceivably, this could be justified on the basis of consent given adequate prior notification and transparency, it is difficult to see how any such processing could be shown to be necessary and of any benefit to the data subject. On the other hand, the potential for harm through breach and misuse is substantial, especially where the communicating enterprise has a material involvement with the data subject, as for instance with finance and utilities providers.

> Unless you genuinely have a customer-wide programme to provide specific and necessary additional or alternative services to people directly affected by Covid-19, and have the privacy, security and medical support necessary to do so appropriately and legally, you should not include these kinds of question in communication with customers.

Staff protection

There can be a legitimate case for soliciting information about a customer's Covid-19 status if your business model involves an in-home visit or other potential physical contact and you wish to protect your employees from possible exposure. However, it's vital in this case to ensure that you use every other available means to mitigate this risk before collecting medical information – including, e.g., offering the customer an option to reschedule at no cost without providing a reason while explaining your purpose. If you do feel it's necessary to get the customer to confirm that no-one in their household is symptomatic before confirming a visit, you should not collect any detailed information, nor connect it to the customer record. Your purpose is solely to determine that the visit should be rescheduled and once this has been done there is no need to retain the data.

> Do not inadvertently build databases of customer medical data in pursuit of protecting your staff. Note that most booking, call-centre and CRM systems are not appropriate for the collection, processing or storage of Special Category data.

Sales targeting

The government has, perhaps unfortunately, encouraged sales targeting on the basis of health information in the specific case of the transfer of the vulnerable persons list to major supermarket chains. There has also been some encouragement of local community sharing of medical status in order to encourage volunteer assistance for those self-isolating or shielding.

The legality of the government's action in transferring the vulnerable persons list was questionable and is likely to be the subject of enquiry after the pandemic is over. There will also be close attention paid to ensuring that the transferred data is not used further once the need for prioritisation of delivery services has passed.

Some enterprises, such as health services companies, may well have legitimate and pre-existing reasons to collect customer health information for marketing and sales targeting purposes and – we should hope – will have the privacy and security controls necessary to do so safely and legitimately.

> However, in most cases, using health information particularly if obtained for another purpose or by way of inference or data enrichment in order to target sales – whether of medical supplies or any other product – will be unlawful and is likely to bring enforcement action even in these unusual times.

Communities

Once an enterprise with strong links into local communities has established for its employees any of the services we discussed earlier – wellbeing, screening, telemedicine or testing – it may be appealing for political or CSR reasons to extend some or all of them to the wider community.

While this may be desirable, it's essential to consider any such extension to be a new processing purpose, and to subject it to proper scrutiny. Often the lawful basis for processing will be different, and it will be harder to prove necessity and proportionality in processing. As a consequence the risks of regulatory action associated with breach or misprocessing will also be greater.

> Community extension of this sort should be done following prior consultation with the local regulator and ideally in conjunction with local or national government. Risks are significantly reduced, although not eliminated, if the extension can be constructed to as to place the enterprise in a processor relationship with a public sector entity as the controller.

About Securys

Securys makes privacy practical for enterprise. We bring legal, cyber security and corporate capabilities to help enterprises address all their stakeholder globally, from customers and employees to suppliers and contractors. All of our consultants are required to obtain and retain IAPP certifications, giving us an unparalleled concentration of knowledge under one roof.

We help our customers look at all of their operations through the lens of privacy, recognising the importance of data subjects across the whole compliance continuum. Our focus is on putting people first, to win trust and avoid harm, not merely on avoiding fines.

We offer a full range of privacy and cyber services including privacy audit, ongoing privacy assurance, privacy by design and privacy-as-a-service. We also act as outsourced DPO for a number of our clients. We go beyond advisory, offering full implementation support; this is how we know our recommendations really are practical.

We specialise in addressing the complex needs of enterprise customers who face both complementary and competing regulation in different territories and who work at scale and change at pace. We combine global reach with local knowledge.

Learn more about Securys and Privacy Made Practical® at www.securys.co.uk

About the authors

Ben Rapp is a career technologist with more than thirty years' experience in information security and data privacy. He is a Certified Information Systems Security Professional with the Information Systems Security Management concentration, a Certified Information Privacy Professional/Europe, a Certified Information Privacy Manager and an IAPP Fellow of Information Privacy; he's also a Chartered Information Technology Professional and a Fellow of the British Computer Society. He previously founded and ran Managed Networks, the leading provider of IT services to the entertainment industry.

Learn more about Ben at https://uk.linkedin.com/in/benrapp

John Lloyd has worked in a wide variety of leadership and governance roles in diverse sectors including media, healthcare and non-profit before joining Securys as a Practice Lead in 2019. He is a Certified Information Privacy Professional/Europe. John is also a trustee of a health charity and a school governor.

Learn more about John at https://www.linkedin.com/in/john-lloyd-4242269/