Employment practices and data protection: information about workers' health

27 October 2022

ico.
Information Commissioner's Office

Contents

Data protection and worker health information

In detail

When might we need to process information about workers' health?

Health information is some of the most sensitive personal information you might process about your workers. Data protection law applies whenever you process information about your workers' health. When we use the terms 'worker' or 'former worker' in this guidance, we mean all employment relationships, whether this includes employees, contractors, volunteers or gig and platform workers.

As an employer, it's likely that there are many circumstances in which you might need to process information about a worker's health. This includes examples such as:

- a questionnaire completed by workers to detect problems with their health;
- sickness absence forms;
- information about their impairment or disability;
- the results of an eye-test taken by a worker using display screens;
- records of blood tests carried out to ensure they have not been exposed to hazardous substances;
- the results of an alcohol or drugs test;
- the results of a fitness to work assessment to determine entitlement to benefits or suitability for continued employment; and

- records of vaccination and immunisation status and history.

Data protection law sets out principles for the collection and use of health information.

Article 4(15) of the UK GDPR gives the following definition of health data:

> "'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."

As this personal data reveals or concerns a person's health, it is a type of special category data with certain extra rules that you must follow. These rules do not prevent the processing of health information, but limit the circumstances in which it can take place.

In an employment context, this covers the collection and use of information about a worker's physical or mental health or condition.

If you want to collect and use information on your workers' health, you should be clear about why you are doing so. You should also be satisfied that you have justified reasons for collecting it. This might be to support your workers by providing flexibility such as reasonable adjustments and equal access, other necessary support or improving health and safety.

You should remember that gathering information about your workers' health will be intrusive and in some cases it may be highly intrusive, depending on the sensitivity of the information. It is reasonable for workers to expect they will need to share a proportionate amount of heath information with you, for example when dealing with sickness absence, occupational health referrals and for other employment-related purposes. However, workers can legitimately expect that employers will respect their privacy when handling their health information.

You should consider whether there are more targeted ways of collecting information about your workers' health that would deliver the outcomes you want while being acceptable to them. For example, rather than testing all your workers for a particular role that requires a certain level of fitness, you might want to use a health questionnaire to select those to be tested.

Data protection law requires fairness, amongst other matters. In general, this means that you should only handle health information in ways that workers would reasonably expect and not use it in ways that have unjustified adverse effects on them. You must be clear about your purposes for processing health information from the start and be transparent about these. You should carefully

consider not only how you can use their health information, but also your reasons why you need to use their information.

You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals. For more details, see Who is responsible for health information and data protection in our organisation? and What do we need to tell workers when processing their health information?.

You can only use the health information for a new purpose if:

- this is compatible with your original purpose;
- you get specific consent from the worker; or
- you have a clear obligation or function set out in law.

You should also be aware of your obligations under employment law, health and safety law and other legislation, as well as any relevant industry standards.

Further reading

Read our guidance on:

Lawfulness, fairness and transparency

Purpose limitation

Special category data

How do we lawfully process the health information of workers?

To lawfully process health information, you must first identify a lawful basis under Article 6 of the UK GDPR. As health information is special category data, it needs a greater level of protection. There are rules covering the use of special category data and you cannot process this type of information unless you meet some additional requirements. This means that in addition to a lawful basis, you also need a condition for processing under Article 9 of the UK GDPR. You may also need to satisfy a condition in Schedule 1 DPA. See What about special category data and conditions for processing? for more information.

Lawfulness also means that you don't do anything with the personal information which is unlawful in a more general sense.

If you process health information about your workers, you must follow these rules.

There are six lawful bases for processing set out in Article 6 of the UK GDPR. You should remember:

- At least one of these must apply whenever you process health information.
- No one basis should be seen as always better, safer or more important than the others, and there is no hierarchy in the order of the list in the UK GDPR.
- How you decide which lawful basis for processing applies depends on your specific purposes and the context of the processing.
- You should think about why you want to process the health information and consider which lawful basis best fits the circumstances.
- You might consider that more than one basis applies, in which case you should identify and document all of them from the start.

You can use our interactive guidance tool to help you decide which lawful basis might apply.

You must determine your lawful basis for processing the health information of workers before you begin this processing under the UK GDPR, and you should document it.

Where your use of health information is likely to result in high risk to your workers you should also carry out a data protection impact assessment (DPIA) before you begin your processing. For more information on DPIAs see What about data protection impact assessments?

Further reading

Lawfulness, fairness and transparency.

Lawful basis for processing

Special category data

Can we rely on worker consent?

Consent is one of the lawful bases for processing personal information. Explicit consent is one of the conditions that can be used to process special category data, such as health information.

The UK GDPR sets a high standard for consent, and people must have a genuine choice over how you use their information. Consent must be unambiguous and involve a clear affirmative action (ie using an opt-in). People must also be able to withdraw their consent as easily as it is to give it.

Explicit consent is not defined in the UK GDPR, but it is not likely to be very different from the usual high standard of consent. The key difference is that explicit consent must be expressly confirmed in a clear statement (whether oral or written), and not by inference from someone's actions.

Explicit consent is the only condition that can apply to a wide range of circumstances. In some cases, it may be the only appropriate condition, depending what you want to do with the health information.

However, it may be difficult for you to rely upon consent to process health data about your workers. This is because, as an employer, you will generally be in a position of power over your workers. They may fear adverse consequences and might feel they have no choice but to agree to the collection of their health information. Therefore, consent is not considered freely given. If the worker has no genuine choice over how you use their information, you cannot rely on consent as a lawful basis or condition for processing.

Example

A company requires its warehouse workers wear a device to monitor their movements for time management and complex stock movement purposes. It has considered whether less intrusive methods would meet these purposes but has decided these don't meet its business needs. The wearable device also has the ability to monitor heart rate. The company asks its workers to consent to the additional collection of heart rate data to measure their fitness levels. As this is health information they also ask for explicit consent. However, the workers may feel compelled to consent, as they don't want to risk their job or be perceived as difficult or having something to hide.

As consent won't be 'freely given', the company cannot rely on consent or explicit consent in this example, given the power imbalance between the employer and worker.

You should avoid relying on consent unless you are confident you can demonstrate it is freely given. This means that a worker must be able to say 'no' without fear of a penalty being imposed and must be able to withdraw their consent at any time.

If you think it will be difficult for you to show that consent has been freely given, you should consider relying on a different lawful basis, such as 'legitimate interests'. See also How do we lawfully process the health information of workers?

However, this does not mean that, as an employer, you can never use consent as a lawful basis. Even where you are in a position of power, there may be situations where you can still show that consent is freely given.

Example

A medical firm offers health screening for its staff, using its own in-house services to test and examine its workers. The firm makes it clear that there is no requirement to take part and participation will not be taken into account for any performative evaluation purposes.

As participation is genuinely optional and there are no adverse consequences to those who do not want to take part, the firm could consider consent as its Article 6 lawful basis. It could also consider explicit consent as its Article 9 condition for processing.

There are also other considerations you need to take into account if you want to rely on consent, such as recording and managing consent. Please see our separate guidance on consent for more information.

What lawful bases might apply if we want to process workers' health information?

We've listed below the most likely lawful bases that might apply to processing the health information of workers in an employment context.

- **Contract**

This lawful basis applies where the processing is necessary for a contract you have with the worker, or because they have asked you to take specific steps before entering into a contract. This is most likely going to apply when you need to process a worker's health information to fulfil your obligations under an employment contract.

- **Legal obligation**

You may be able to rely on this lawful basis where you need to process the health information of a worker to comply with the law (although this does not include contractual obligations). For example, where you might be required to report 'specified injuries' to the Health and Safety Executive, under RIDDOR 2013.

- **Legitimate interests**

This may apply if the processing of the health information is necessary for your legitimate interests or the legitimate interests of a third party. This won't apply if there is a good reason to protect the worker's personal information which outweighs those legitimate interests. An example of where legitimate interests

may apply could be where you need to process a disabled worker's health information to make their work environment more accessible to them.

- **Other lawful bases**

In exceptional circumstances, you may be able to rely on the vital interests lawful basis where you need to process the health information of a worker to protect their life, or the life of another person. This lawful basis is very limited in its scope and generally only applies to matters of life and death.

Remember, it is your responsibility to decide what lawful basis is most appropriate for your health processing. If you can meet the criteria for a specific lawful basis, then you are likely to be able to rely on it.

What about special category data and conditions for processing?

As explained above, when processing special category data such as health information, as well as identifying a lawful basis under Article 6, you also need a condition for processing under Article 9. There are 10 conditions for processing special category data. Five of these require you to meet additional conditions and safeguards set out in Schedule 1 of the DPA 2018.

The most likely conditions relevant to processing health information of workers in an employment context are:

- **Employment, social security and social protection law**

This condition is particularly relevant for employers, for example where you are:

- ensuring health, safety and welfare of workers; or
- maintaining records of statutory sick pay and maternity pay.

Your purpose must be to comply with employment law, or social security and social protection law. You need to be able to identify the legal obligation or right in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable employment obligations or rights.

This condition does not cover processing to meet purely contractual employment rights or obligations.

You must be able to justify why processing of this specific information is 'necessary'. It must be a reasonable and proportionate way of meeting specific rights or obligations. You must not obtain or use more information than you need.

If you are relying on this condition, you also need to meet the associated condition set out in Part 1 of Schedule 1 of the DPA 2018. This condition also requires you to have an appropriate policy document in place.

- **Legal claims or judicial acts**

You may be able to rely on this condition to permit you to process health information if the processing is necessary to establish, exercise or defend legal claims. This might be the case where a worker is suing their employer over an incident that affected their health.

Example

An employer is being sued by one of its workers following an accident at work. The employer wants to pass the details of the accident to its solicitors to obtain legal advice on its position and potentially to defend the claim. The information about the accident includes details of the worker's injuries, which qualify as health information. The purpose of the disclosure is to establish its legal position and to defend the claim.

You must be able to justify why processing of this specific information is 'necessary' to establish, exercise or defend the legal claim. The use of this information must be relevant and proportionate, and you must not obtain or use more information than you need.

You can only rely on the legal claims element of this condition, as the judicial acts element only applies to courts acting in their judicial capacity.

- **Substantial public interest**

This condition allows you to process health information, if this is necessary for reasons of substantial public interest, as set out in UK law.

To rely upon this condition, you will need to meet one of the specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018. You must also have an '[appropriate policy document]' in place for almost all of these conditions. See 'Is there anything else we need to consider?' below for more details.

The most likely substantial public interest conditions relevant for processing worker health information are:

- Statutory and government purposes
- Safeguarding of children and of individuals at risk

This list isn't exhaustive and if you intend to rely on any substantial interest conditions, you also need to look at the details of the specific conditions in the legislation to determine what condition is most appropriate to your purpose.

- **Other conditions**

You may also find that vital interests or explicit consent apply in some limited circumstances, with similar considerations as the lawful bases of consent and vital interests discussed above. Please see the section Can we rely on worker consent? for more detail on consent.

Is there anything else we need to consider?

If you are relying on a Schedule 1 condition for processing, many of these also require you to have an appropriate policy document in place. This acts as part of the additional safeguards that are necessary for the processing to take place. See our separate guidance for more information on what is an appropriate policy document. We have also produced a template you can use.

Remember that you need to determine your condition for processing before you begin the processing and you should document your decision, along with your lawful basis.

Further reading

Lawfulness, fairness and transparency.

Special category data

Substantial public interest conditions.

How do we limit how much health information we collect?

You must not collect more health information than you really need for your stated purpose. What you do collect should be relevant, and adequate to properly fulfil that purpose. This links closely with the storage limitation principle where you should consider how long you need to keep the information and why (see How long should we keep worker health information? below).

In general, you should collect as little health information about as few workers as possible. It's likely employers will need to obtain at least some health information about their workers during the normal course of their employment. How much health information you collect will depend on what is necessary for certain job roles. Some roles might require you to collect more detailed health information about your workers, such as those working in hazardous environments, workers whose jobs require high levels of physical fitness, or

those dealing with clinically vulnerable individuals. This will often be for health and safety reasons. You should collect more detailed health information in areas of highest risk only. Consider whether you can collect health information from only a few individuals whose jobs are critical to safety or who work in a hazardous environment.

Example

An employer decides to use health questionnaires for its workers to ensure they are fit to work in a demanding physical job role. The employer ensures that only information that is really needed is collected from its workers and that the health questionnaire is designed to ensure it only collects relevant information.

It is good practice for questionnaires to be designed by health professionals. This also means they should be interpreted by those who are qualified to draw meaningful conclusions from the information supplied by the worker.

You should check any questionnaire you use to ensure it complies with the Equality Act 2010 or section 75 of the Northern Ireland Act 1998.

Example

An employer commissions a medical report on a worker who is off work due to a long term sickness absence. The employer only asks for information on the worker's fitness for continued employment in their role. They don't ask the medical report author to provide medical details of the worker's condition. The author is asked to provide an assessment of whether or not the worker is fit to return to employment, whether they should be redeployed, or whether adjustments need to be made to the workplace to accommodate their condition.

Example

An employer needs access to specific information from a worker's medical record. The employer does not ask the worker to consent to the disclosure of their entire medical record, as this contains more information than the employer needs. Instead the employer only seeks the disclosure of the whole record, or substantial parts of it, where this is genuinely necessary. Where information from a GP or other medical professional is needed, they are asked specific, relevant questions to elicit the information needed by the employer.

Where an employer needs to obtain a report from a worker's GP or other medical practitioner who has been responsible for the care of the worker, the employer ensures that it meets the requirements of the Access to Medical Reports Act 1988 or the Access to Health Records (Northern Ireland) Order 1993.

You must not collect health information purely on the chance that it might be useful in the future. However, you could hold information for a foreseeable event that might never occur if you can justify it.

Example

An employer holds details of the blood groups of some of its workers who do hazardous work. The employer has safety procedures in place to help prevent accidents so it may be that this information is never needed, but it still needs to hold this information in case of an emergency.

However, it would be excessive to hold details of the blood groups of the rest of the workforce, who aren't involved in hazardous work.

You should remember that, as an employer, your interest is mainly in knowing whether a worker is or will be fit to work. As far as possible, it should be left to medical professionals to have access to and interpret detailed medical information for you. See also What about occupational health schemes? and What about medical examinations and testing?

You should also be aware that workers have a right to rectification and a right to erasure.

Further reading

For more information see our guidance on data minimisation.

What do we need to tell workers when processing their health information?

Data protection law requires fairness and transparency, and provides a right for people to be informed about how their personal information is being used and why.

Transparency is fundamentally linked to fairness. Transparent processing is about being clear, open and honest with your workers. You must let your workers know that information about their health is being collected and why, who will have access to it, and in what circumstances. You're unlikely to ever be able to justify gathering information about workers' health covertly.

You must include specific information about your processing of health information in your privacy information for your workers. It's important that you tell people about your processing in a way that is easily accessible and easy to

understand, using clear and plain language. There are a range of ways you can provide this privacy information. You could provide it:

- as part of your staff privacy notice on your organisation's intranet;
- as part of your general data protection policy;
- as separate privacy information in a worker handbook;
- using 'just in time' notices if using online workshops, platforms or tools where health data might be collected or shared with others;
- as a general notice on a staff notice board; or
- by sending a letter or email to workers.

What method you use and the most effective way of giving privacy information to your workers will depend on the nature of your organisation and what way fits best with your needs.

Where you are taking a specific action, for example where a worker is to undergo a medical test, ensure the worker is fully aware what, why and how much information is to be collected, and what rights they have under data protection law. If they are referred to a doctor or nurse, it is important that they know what sort of information you will receive as a result. See also What about occupational health schemes? and What about medical examinations and testing?

Further reading

Read our guidance on lawfulness, fairness and transparency and the right to be informed for more detail on your transparency obligations and the privacy information you must provide to individuals.

How long should we keep workers' health information?

You must not keep personal information for longer than you need it. Therefore, you need to consider how long you need to keep worker health information, as well as the health information of former workers, and be able to justify doing so. This depends on your purposes for holding the information.

Where you are processing health information, to comply with documentation requirements you must record your retention schedules. It is good practice to have a retention policy, wherever possible.

You should also periodically review the health information you hold, and erase or anonymise it when you no longer need it.

Example

You have collected general health information about a worker during the course of their employment. Once they have left your organisation, you review whether you need to retain that information now they are no longer employed by you. You delete any unnecessary information, subject to any other legal obligations you may have around retaining employment records.

You also need to carefully consider any challenges to your retention of worker health information. Workers have a right to erasure if you no longer need the information for the purposes for which it was collected.

You should consider any legal or regulatory requirements. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information on aspects of health and safety. If you keep health information to comply with a requirement like this, you will not be considered to have kept the information for longer than necessary.

This principle closely relates to the data minimisation principle (see How do we limit how much health data we collect? above).

Further reading

Read our guidance on storage limitation

How do we keep workers' health information accurate and up to date?

The UK GDPR requires personal information be accurate and, where necessary, kept up to date (the accuracy principle). You should take all reasonable steps to ensure the health information of workers you hold is not incorrect or misleading as to any matter of fact.

You may need to keep the health information updated, although this depends on the nature of the information and what you are using it for. For example, if you hold data about a worker's blood type, the data itself will not change. However, if you need to keep records of details that can change over time, such as a worker's hearing level these may need to be updated. It probably worth asking the worker concerned to review and confirm any changes.

If you discover that health information is incorrect or misleading, you must take reasonable steps to correct or erase it as soon as possible.

You must carefully consider any challenges to the accuracy of health information by your workers.

This principle has clear links to a worker's right to rectification and their right to erasure.

Further reading

Read our guidance on accuracy.

How do we keep the health data of workers secure?

The UK GDPR requires that you have appropriate security measures in place to protect the health information of your workers. This is the 'integrity and confidentiality' principle of the UK GDPR – also known as the security principle.

You should keep information about workers' health particularly secure. For example, limiting access to only those who need to see it, such as password protecting it. If a physical record exists, you should keep it in a sealed envelope in the worker's file or in a locked cabinet.

The level of security must be appropriate to the nature of the information to be protected and harm that might result from misuse or loss. Given that health information is special category data, the level of security required is a high one. Unless you apply a particularly high level of security to all employment records, it is likely that health information about your workers will need to be singled out for special treatment.

Depending on the nature of your organisation, it may be possible to keep information about your workers' health on a separate database or system, or subject to separate access controls. If you use physical records, it may be possible to separate health information from the other contents of a worker's personnel file (such as by putting it in a sealed envelope).

You should also consider who has access to worker health information. The principle of 'need to know' should be strictly applied. As far as possible, access to information on medical conditions should be limited to health professionals, such as doctors and nurses. Managers should only have access where it is necessary for them to undertake their management responsibilities and this should be limited to only the information they need to meet their obligations. This can very often be limited to information about a worker's current or likely future fitness to work and may be less information than a doctor or nurse may need to make an assessment of the worker. In some cases, a manager may need to know more about a worker's state of health to protect that worker or others.

When you are reviewing your information management systems, you should consider data protection by design and by default, so that data protection is built in to your systems.

Further reading

We have produced separate guidance on security.

What about automated decision making and health information?

Employers may sometimes want to use automated decision-making in relation to their workers. This is where a decision is made by automated means without any human involvement.

These decisions often involve profiling of people, although they do not have to. In an employment context, profiling might be used to analyse or predict aspects of a worker's performance.

Article 22 of the UK GDPR restricts you from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on people. Where you want to use special category data, the restrictions are stronger. This means you must not use your workers' health information in any automated decision-making systems unless:

- you have the worker's explicit consent; or
- the processing is necessary for reasons of substantial public interest.

If you are able to meet one of these, there are additional requirements you must satisfy, including allowing workers to request human intervention or to challenge a decision. As this is considered high-risk you are required to carry out a DPIA.

If Article 22 does not apply, for example, because there is meaningful human involvement, then you can continue to carry out profiling and automated decision-making. However, you must still comply with the UK GDPR principles and identify and record your lawful basis for the processing.

You need to have processes in place so people can exercise their rights.

People have a right to object to profiling in certain circumstances. You must bring details of this right specifically to their attention.

Further reading

Rights related to automated decision making including profiling

Automated decision-making and profiling

What about data protection impact assessments?

A data protection impact assessment (DPIA) is a process to help you identify and minimise data protection risks. An effective DPIA allows you to identify and fix problems at an early stage, bringing broader benefits for both individuals and your organisation.

Data protection law requires you to do a DPIA before you begin any type of processing that is "likely to result in a high risk". This includes some specified types of processing. There are also other circumstances where you must do a DPIA and in some cases you must consult the ICO before you can begin processing.

It is good practice to carry out a DPIA given the sensitive and potentially intrusive nature of processing the health information of workers and, in some cases, it may be a requirement depending on the processing you want to do. Throughout this guidance, we highlight issues we recommend are considered as part of your DPIA. Where a DPIA isn't required, a risk assessment is still a useful tool to help you identify any potential issues with your proposed use of health information.

Further reading

For more information on DPIAs, including when to do one and what to consider, and a DPIA template, read our separate guidance.

Who is responsible for health information and data protection in our organisation?

Accountability is one of the key principles in data protection law. The accountability principle requires you to take responsibility for what you do with personal information and how you comply with the other principles.

You must have appropriate measures and records in place to be able to demonstrate your compliance with your data protection obligations. This doesn't just include compliance with the principles (as explained in the preceding sections) but also your other obligations, such as taking a 'data protection by design and default' approach, documenting your processing activities, and carrying out data protection impact assessments (DPIAs) for uses of personal information that are likely to result in high risk. For more information, see the guidance on accountability and governance.

You should identify who within your organisation has responsibility to authorise or carry out the collection of information about your workers' health. You should ensure they are aware of your organisation's policies and procedures.

You should also ensure they are made aware of data protection law. If they lack proper authority and necessary training, this could lead to a risk of non-compliance. For example, when deciding to collect health information, or when introducing medical testing. It is also important to consider any obligations under other laws, such as employment law and health and safety legislation.

Ultimately, your organisation, as the controller, has responsibility for data protection compliance. If you use any processors when processing health information on your behalf, you need to ensure you have a written contract in place with them. See our separate guidance on controllers and processors for more information.

If you have a data protection officer, you should involve them in any decisions relating to your processing of health information.

You also need to be aware of the data protection rights workers have when you are processing their health information.

Further reading

We have produced the Accountability Framework, which can help any organisation, whether small or large, with their obligations. You may wish to use the Framework to help you assess your organisation's accountability.

How do we handle sickness and injury records?

In detail

What about sickness, injury and absence records?

This section of the guidance considers some of the key data protection issues when employers handle sickness, injury and absence records.

In this guidance, we distinguish between sickness, injury and absence records:

- **Sickness record**

This is a record which contains details of the illness or condition responsible for a worker's absence.

- **Injury record**

This contains details of the injury suffered by a worker (which may or may not cause absence). Many employers keep accident records, but such a record will only be an 'injury record' if it includes details of the injury suffered by an identifiable worker.

- **Absence record**

This is a record that may give the reason for absence as 'sickness' or 'accident' but does not include any reference to specific medical conditions. It may be preferable to use absence records instead of sickness records where this is practical, as generally these will be less intrusive to workers' privacy. A simple absence record, without any details of a worker's health condition is not likely special category data. See also How should we limit access to sickness, injury and absence records of individual workers? below.

Can we process sickness and injury records?

Data protection law does not prevent you from keeping sickness and injury records about your workers. Clearly, these types of records are necessary for an employer to review the ability of workers to undertake their work, and for other purposes such as identifying health and safety hazards at work, and the payment of health-related benefits to workers.

However, you should make sure that sickness and injury records aren't used in a way workers would not expect. It is important to make it clear to those who have access to sickness records what they can and cannot do with them, as well as whether full access is appropriate. This links with your fairness and transparency obligations.

Example

Revealing sickness absences to all workers as part of a 'league table' is an example of where it might be inappropriate and not within someone's reasonable expectations of how their sickness information might be handled.

No 'league tables' of sickness absences of individual workers should be published where everyone can see a person's sickness, injury or absences. This would be intrusive to workers' privacy and disproportionate to any managerial benefit.

Instead it would be permissible to publish totals of sickness absence by department or section as long as individual workers are not identifiable.

You may also need to check whether your purposes for using sickness records may be further restricted by other legislation, such as the Equality Act 2010 or section 75 of the Northern Ireland Act 1998.

How do we lawfully process sickness and injury records?

Sickness and injury records include information about workers' physical or mental health. The holding of sickness or injury records therefore involves the processing of special category data.

It is part of your accountability obligations to identify a suitable lawful basis and condition for processing. However, for sickness and injury records you can likely rely on legitimate interests or legal obligation as your lawful basis, and the employment law condition for processing. An employer is likely to need to process sickness records to meet various employment law obligations, such as health and safety and disability obligations, and to avoid unfair dismissal on the grounds of absence. It is also likely to be both in the employer's and the worker's interests to keep such records.

Consent as a lawful basis and explicit consent as a condition for processing are unlikely ever to be appropriate as a basis for processing sickness records. This is because a worker is unlikely to be able to freely consent to the processing, especially in cases where an employer may use sickness absences in potential disciplinary proceedings. As already noted above, employers also have obligations under employment law which means the worker won't have any real choice to consent.

For more information on lawfully processing health information, please see How do we lawfully process the health information of workers?

How should we store sickness and injury records?

Where possible, you should keep sickness and injury records containing details of a worker's illness or medical condition separate from other less sensitive information, for example a simple record of absence. As noted above, a record of absence does not contain details of a worker's health condition. This helps ensure that information on a worker's health is not accessed when only information on absence or the circumstances of an accident at work is needed. See How should we limit access to sickness, injury and absence records of individual workers? below for more information.

It is a good idea to review how your organisation's sickness and accident records are currently kept. If necessary, change the way information on sickness and accidents is kept.

You should ensure appropriate measures are taken to keep sickness and injury records secure, especially given the sensitive nature of the information. This can be done by keeping the sickness record in a specially protected computer file, perhaps using encryption, or if you use physical records, in a sealed envelope stored in a locked filing cabinet.

How should we limit access to sickness, injury and absence records of individual workers?

You must not make the sickness, injury or absence records of individual workers available to other workers unless it is necessary for them to do their jobs.

Managers are usually provided with information about those who work for them where this is necessary for them to carry out their managerial roles. For example, it would be permissible for a manager to access the record of a worker's sickness to investigate repeated or long-term absence. You should make sure that managers are aware of the sensitive nature of sickness and injury records and to handle them appropriately.

How much personal information from sickness records should be accessed depends on the purpose of the processing.

You should make it clear to those accessing both sickness, injury and absence records of when it is and is not necessary to access the full sickness or injury records.

Example

An organisation has a reasonable adjustments 'passport' scheme in place. This stores details of an individual worker's health condition and reasonable adjustments that are needed because of their health condition. This enables the organisation to keep a record of the worker's agreed adjustments, which can be accessed by their new manager if they move to a different team.

The organisation needs to inform its facilities team of the reasonable adjustments necessary to the individual's workstation. The facilities team are able to see what reasonable adjustments the worker requires so they can set up the workstation as needed. However, it is not necessary for them to see details of the workers' health condition.

You should not use sickness or injury records when information only about the length of an absence is needed. Similarly, you should not use sickness records for a particular purpose when records of absence could be used instead, for example, when only information on absence or the circumstances of an accident at work is needed.

Example

When an employer is calculating a benefit, it may only be necessary for admin staff to see the length of a worker's absence rather than the nature of the sickness responsible for their absence.

Can we share information from sickness or injury records?

You should only share information from sickness or injury records about an identifiable worker's illness, medical condition or injury with third parties where:

- there is a legal obligation to do so;
- it is necessary for legal proceedings; or
- the worker has given explicit consent to the sharing.

Make sure that all those who deal with workers' sickness or injury records are aware of the circumstances where there may be a legal obligation to share the information.

It is important to remember that this does not stand in the way of sharing the number of days of a worker's absence, for example when giving a reference.

See the section When can we share worker health information? for more information. This also addresses circumstances involving disclosing information about a worker's health to other workers.

What about occupational health schemes?

In detail

This section provides advice for employers with occupational health schemes. It does not provide detailed professional guidance to doctors, nurses and others involved in such schemes.

What must we tell workers when using an occupational health scheme?

Remember that workers have a right to be informed how you use their personal information and why. It is part of your transparency obligations to be clear about this from the outset. This includes when you may share their information with external occupational health providers and what information you may get back from them.

You must set out clearly to workers, preferably in writing, how you intend to use information they supply in the context of an occupational health scheme, who it might be made available to and why. You should also be transparent about what data protection rights individual workers have around the use of their information and the reports that are produced. It is particularly important to inform workers of the circumstances, if any, when their line manager will have access to the information they supply to a health professional.

Unless told otherwise, workers are entitled to assume that information they give to a doctor, nurse or other health professional will be treated in confidence and not passed to others.

Further reading

Right to be informed

How should we limit who has access to medical information about workers?

Medical details about individual workers should only be made available to managers where it is necessary to allow them to discharge their management responsibilities. This type of access should be kept to a minimum. As far as possible, an occupational health advisor should hold the medical information about a worker, only telling the worker's manager the results of the health assessment, for example whether or not there's a legitimate reason for a worker's absence from work.

Depending on the nature of your organisation, your HR department may well be involved in the referral process of a worker to an occupational health provider. It might have some access to that worker's health information, particularly if changes to their workplace are needed as a result. The key point is that only information that is genuinely needed for those to carry out their roles effectively should be made available to them.

You should remember that the sharing of medical information given by a worker to an occupational health practitioner, or other health professional, is restricted not just by data protection law, but also by a duty of confidence. Generally, you will need to obtain explicit consent for the release of such information to non-medical personnel.

You should also consider whether you need to comply with any guidance from relevant professional bodies and regulators, such as the GMC or Health and Care Professions Council.

Other resources

General Medical Council

Health and Care Professions Council

Faculty of Occupational Medicine

What about workers' confidential communications with health professionals?

You must not compromise any confidentiality of communications between workers and health professionals in an occupational health service.

If workers are allowed to use work telephones or email accounts for confidential communication with their occupational health service, you should not compromise this confidentiality by monitoring the contents of these communications.

If your systems are set up in such a way that a confidential conversation or other communication is unintentionally picked up, information relating to that conversation or communication should be deleted at the earliest opportunity and no record should be kept of it.

It may be beneficial to ask your workers to mark private communications such as emails sent via work systems appropriately to help you avoid reading confidential messages. For example, you could ask your workers to mark them 'non-work', 'private' or 'union business' to help you avoid reading confidential messages.

Are occupational health providers controllers or processors?

If an occupational health provider is processing personal information in its professional capacity, with its own medical professional obligations, it is likely to be acting as the controller, rather than as a processor.

Example

Employer A contracts its occupational health provision to Company B. Company B is a professional occupational health provider and its providers comply with their own medical obligations. Company B determines the purposes of the processing of the health information of workers referred to it. Company B is the controller.

This also means that the occupational health provider must comply with its data protection obligations as a controller. This includes responding to information rights requests made by workers, such as subject access requests.

It is important to remember the employer will be the controller for any personal information about its workers it obtains for its own purposes from the occupational health provider.

It is a good idea to tell your workers who is in control of what health information, and who to direct any information rights requests to.

If you use an occupational health provider regularly you should consider implementing a data sharing agreement with the provider. For more information, please see our separate guidance on data sharing agreements.

Further reading

Controllers and processors

Contracts

What do we need to do when requesting a worker's medical file as part of an occupational health referral?

If you need a report from a worker's GP or any other medical practitioner responsible for their clinical care, then the Access to Medical Reports Act 1988 or the Access to Health Records (Northern Ireland) Order 1993 applies. Although this legislation is not part of data protection law, the information you receive from the report is subject to data protection law.

You should not normally ask workers to consent to the disclosure of their entire medical record or other comprehensive care and treatment records (such as those held by a hospital). This is because you are highly unlikely to need to see their entire record. See also How do we limit how much health information we collect?

Other resources

Access to Medical Reports Act 1988

Access to Health Records (Northern Ireland) Order 1993

What about medical examinations and testing?

In detail

Why might we want to obtain information from medical examinations and testing?

There may be several reasons why you want to collect health information from the testing and medical examination of workers. This will often be for health and safety reasons, but you may also want to enforce your organisation's rules and standards (for example, through drugs and alcohol testing). Employers may also want to carry out medical examinations and testing when assessing the suitability of potential workers during a recruitment process (see Can we use medical examinations and testing as part of our recruitment process?).

You can collect such information if you are satisfied that it is a necessary and justified measure to:

- prevent a significant risk to the health and safety of the worker or others;
- determine a particular worker's fitness for carrying out their job;
- determine whether a worker is fit to return to work after a period of sickness absence, or when this might be the case;
- determine the worker's entitlement to health-related benefits eg sick pay;

- prevent discrimination against workers on the grounds of disability or assess the need to make reasonable adjustments to the working environment; or
- comply with other legal obligations (such as the obligation on an employer under the Control of Asbestos of Work Regulations 2002 or the Control of Asbestos at Work Regulations (Northern Ireland) 2003 to keep workers who are exposed to asbestos under adequate medical surveillance).

You may also want to test workers as part of an occupational health and safety programme. However, this should only take place where workers have a free choice to participate and the potential consequences of doing so have been clearly explained to them.

Workers employed on overseas contracts may be expected to undergo a degree of medical examination and testing that is substantially more intrusive than that carried out on workers in the UK. For example, workers contracted to work in certain countries may be exposed to particular risks or there may be a legal requirement for testing in the country concerned. You should make sure that you make workers aware of any examination or testing that they will be expected to undergo at an early stage.

Why should we consider if we want to introduce medical examinations and testing?

You should record the purpose of the programme of examination or testing of workers is to be introduced and the lawful basis and condition for processing that can be satisfied. You may wish to do this as part of your data protection impact assessment (DPIA).

You should also document:

- who will be tested or examined;
- what precisely they will be tested or examined for;
- the frequency of testing or examinations; and
- the consequences of a positive or negative test or the result of an examination.

It is also important to consider whether there are any less intrusive ways of meeting your objectives as an employer. This might mean, for example, collecting information via a health questionnaire either as a first stage or as an alternative to a medical examination.

Further reading – ICO guidance

Data protection impact assessments

Can we use medical examinations and testing as part of our recruitment process?

Medical examination and testing are intrusive and should only be used to obtain information where this is necessary to meet your purposes for carrying these out. This means employers should not subject all applicants for a job, or even those shortlisted, to examination or testing. You should only obtain information through medical examination or testing of applicants at an appropriate point in the recruitment process. This is probably going to be where there is a likelihood of appointing them, such as where you only intend to appoint them, subject to satisfactory examination or test results.

You must also be satisfied that the testing or examination is a necessary and justified measure to:

- determine whether the potential worker is fit or likely to remain fit to carry out the job in question;
- meet any legal requirements for testing or examination; or
- determine the terms on which a potential worker is eligible to join a pension or insurance scheme.

You should record your purpose for introducing the examination or testing, and your lawful basis and condition for processing. You can do this as part of your DPIA.

Remember to first consider less intrusive ways of meeting your objectives. For example, using a health questionnaire as an alternative to medical examination or as a means to select those required to undergo a more detailed examination.

You should make it clear early on in the recruitment process that people may be subjected to medical examination or testing once there is a likelihood that they will be appointed.

Decisions on a worker's suitability to work are management decisions but the interpretation of medical information should be left to a suitably qualified health professional.

How should we limit the purpose of the examination or testing and the information we obtain?

You must be clear from the outset about the purpose or purposes the testing or examination is being carried out for, including what substances or conditions are being looked. You can consider these issues as part of a DPIA, which can help you determine whether a medical examination or testing is a proportionate response to a particular problem you have identified.

Testing or examination should be designed to only reveal information relevant to your purpose for carrying it out.

You should not use an existing sample, test result, or other information obtained through a medical examination or test for a purpose other than that for which it was originally collected.

If you want to carry out a different test on an existing sample that the worker has not been told about and has not consented to, you must tell the worker about your intention to carry out additional testing. You must also obtain the worker's freely given consent for this different test.

Example

It would be unfair to the worker to test a blood sample for the presence of alcohol when the worker has only been told the sample would be tested to check for the presence of a particular chemical to which the worker might have been exposed.

It would also be unfair to obtain information by performing a drug test on a sample of a worker's hair without the worker's knowledge.

How do we ensure testing is appropriate?

You should make sure that the information you collect from testing is designed to ensure safety at work rather than to reveal the illegal use of substances in a worker's private life. This is because testing workers for drugs or alcohol is intrusive and very few employers will be justified in testing to detect illegal use rather than on safety grounds. However, testing to detect illegal use may, exceptionally, be justified where illegal use would:

- breach the worker's contract of employment, conditions of employment or disciplinary rules; or
- cause serious damage to the employer's business, for example by substantially undermining public confidence in the integrity of a law enforcement agency.

Before obtaining any information from drug or alcohol testing you should ensure the benefits justify any adverse impact on your workers, unless the testing is required by law. You should also consider the efficacy of the testing technique you wish to use to ensure the accuracy of the information you collect about your workers. See How do we ensure testing is of a good standard and quality? below. You can do this via a DPIA.

You need to take particular care when carrying out a DPIA on whether the collection of information through drug testing is justified on health and safety grounds. You should take into account the following points:

- Your interest as an employer is usually in detecting drug use that puts at risk the safety of those to whom you owe a duty of care. This can arise from drugs that are legal as well as illegal. You shouldn't test merely to find evidence of the use of illegal drugs.
- The drug testing you use must address the risk. It must be capable of providing real evidence of impairment or potential impairment at work that is sufficient to put the safety of others at risk.
- Other than in the most safety critical areas, regular drug testing is unlikely to be justified unless there is a reasonable suspicion of drug use that has an impact on safety.
- Drug testing must provide significantly better evidence of impairment that puts safety at risk than less intrusive alternatives, such as a test of cognitive ability.
- You are more likely to justify testing after an incident involving a worker's conduct where there is a reasonable suspicion of drug or alcohol use, rather than by carrying out random testing.

How much personal information should we collect from testing?

You should minimise the amount of personal data you obtain from testing for the presence of drugs and alcohol in your workers.

You should only use drug or alcohol testing where it provides significantly better evidence of a worker's impairment than other less intrusive means. You should base any testing on reliable scientific evidence of the effect of particular substances on workers. You should limit testing to those substances and the extent of exposure that will have a significant bearing on the purpose(s) for which testing is conducted.

You can do this by limiting the number of substances being tested for, or by using tests that only detect recent exposure to the substances being tested for. A variety of techniques for carrying out alcohol and drug testing are available to employers. They vary in the level of intrusiveness, depending on the range of substances that can be detected and the time scales involved. For example, some tests are only designed to detect the use of a particular drug within the previous eight-hour period, whilst others are designed to detect the use of a wide range of substances over a much longer period. Employers intending to carry out testing should use the least intrusive methods available to deliver the benefits that the testing is intended to bring.

There are tests, computer programs and equipment that can be used to measure hand-eye coordination and response time. These do not involve any invasive medical procedures and so are more justifiable for tests in the first instance. Assisted performance tests may be more reliable for the employer in providing evidence of impairment and less intrusive for the worker.

How do we select workers for testing?

When you select workers for testing, you should ensure that the criteria used are justified, properly documented, adhered to and are communicated to workers.

It is generally unfair and deceptive to lead workers to believe that testing is being carried out randomly if, in fact, other criteria are being used.

If you do carry out random testing, ensure that it is carried out in a genuinely random way. See What about random testing? below.

If other criteria are used to trigger testing, you should ensure workers are aware of the true criteria that are being used.

Example

You suspect that a worker's performance is impaired as a result of drug or alcohol use. Your drugs and alcohol policy makes it clear that where a worker's performance appears to be impaired and is posing a risk to the health and safety of the worker and others, that person is required to undergo testing for evidence of impairment. You record the decision that the worker is required to undergo a drugs and alcohol test. You also record the results of the test.

What about random testing?

Collecting personal information by testing all workers in an organisation will not be justified if in fact it is only workers engaged in particular activities or roles that pose a risk.

You should instead limit the collection of information through random testing to those workers who are involved in safety critical roles that you consider require testing.

Even in safety-critical businesses such as public transport or heavy industry, workers in different jobs will pose different safety risks through their use of alcohol or drugs, depending on the type of work they carry out. Therefore collecting information through the random testing of all workers will rarely be justified.

Example

A train driver or signal engineer whose actions are impaired through exposure to alcohol or drugs would generally pose a significantly greater safety risk than would a ticket inspector or rail enquiries clerk. This difference in risk should be reflected in your DPIA. You shouldn't test ticket inspectors or rail enquiries clerks simply on the basis that fairness somehow requires that if drivers or signal engineers are tested, they should be tested as well.

What should we tell workers about examinations and testing?

You must ensure that workers are fully aware when testing is taking place or where medical examinations are required, as part of your fairness and transparency obligations.

Example

Your organisation has a policy of testing workers for drugs and alcohol exposure for health and safety reasons.

As part of your transparency obligations, you should tell them:

- when drugs or alcohol testing may take place;
- what drugs they are being tested for;
- the alcohol level at which they may be disciplined when being tested for alcohol; and
- what are the possible consequences if they breach the policy.

You may wish to explain your drug or alcohol policy in a staff handbook, or other easily accessible source.

You should not conduct testing on samples collected without the worker's knowledge. For example, it would be deceptive and misleading to workers if an attempt was made to obtain information by collecting samples covertly, or by testing existing samples in a manner that workers have not been told about. Where this type of testing involves the processing of personal information it is unlikely to comply with data protection law as it would be unfair to the worker concerned. Covert medical testing is unlikely to ever be justified and it is difficult to envisage circumstances arising without the police being involved.

If you are testing workers to enforce your organisation's rules and standards, you must make sure that these are clearly set out to your workers, for example, in document setting out your policy. You should set out:

- the circumstances in which medical testing may take place;

- the nature of the testing;
- how you intend to use the information obtained; and
- the safeguards in place for the workers that are subject to it.

You need to explain similar considerations if you want workers to undergo medical examinations.

Can we retain information obtained from medical examination or testing?

You should permanently delete information obtained from medical examination or testing that is not relevant for the purpose(s) for which the examination or testing is undertaken.

Example

Information obtained during a drug test that happens to indicate that a worker is pregnant should not be recorded or used. In addition, tests should be designed, as far as possible, to not detect this in the first place.

If you do need to retain medical information obtained from examination and testing (such as where it necessary for the operation of an occupational health service), it should be kept securely and confidentially in an appropriate storage system.

How do we ensure testing is of a good standard and quality?

It is important to ensure that any information is only obtained through testing that is:

- of sufficient technical quality to support any decisions or opinions that are derived from it;
- subject to rigorous integrity and quality control procedures; and
- conducted under the direction of, and positive test results interpreted by, a person who is suitably qualified and competent in the field of drug testing.

To achieve this, you should use a professional service with qualified staff that meets appropriate standards. You should also ensure that workers have access to a duplicate of any sample taken to enable them to have it independently analysed to check the accuracy of the results. You should not assume that the tests are infallible. You should be prepared to deal properly with any disputes arising from their use.

The reliable interpretation of test results can require a high level of technical expertise. You may need to seek appropriate technical advice and use an

approved laboratory to analyse samples to satisfy your legal duty to ensure results are adequate for the purpose(s) of the testing. It is not necessary to employ health professionals to undertake tests for alcohol using breath analysis equipment.

Although sample kits that can be used to test for various substances are available over-the-counter, you should not assume that the tests are infallible. Some test kits may fail to differentiate between an illegal drug and a legitimate pharmaceutical, or between a pharmaceutical that causes impairment and one that does not.

What about genetic testing?

In detail

Can we use genetic testing on our workers?

Genetic testing is likely to result in the processing of genetic data about workers. Genetic data is a type of special category data and so all the usual considerations about processing this category of personal information would apply. For more information on what is genetic data, read our separate guidance.

Genetic testing has the potential to provide employers with:

- information predictive of the likely future general health of workers; or
- with information about their genetic susceptibility to occupational diseases.

However, genetic testing is still under development and in most cases has an uncertain predictive value. It is rarely, if ever, used in an employment context. It is difficult for employers to justify demanding that a person should take a genetic test as a condition of employment.

You should not use genetic testing to obtain information that is predictive of a worker's future general health. To obtain information this way is too intrusive. The predictive value of the information is also insufficiently certain to be relied on to provide information about a worker's future health.

Genetic testing should therefore only be introduced after very careful consideration, if at all.

Can we ask a worker to disclose the results of a previous genetic test?

You must not insist that a worker discloses the results of a previous genetic test to you. It is important that workers are not put off taking genetic tests that may be beneficial for their health care by the fear that they may have to disclose the results to their current or future employer.

You can ask for information that is relevant to your health and safety or other legal duties but the provision of the information should be voluntary.

Are there any circumstances we can use information from genetic testing?

You should only use genetic testing to obtain information as a last resort where:

- it is clear that a worker with a particular detectable genetic condition is likely to pose a serious safety risk to others; or
- where it is known that a specific working environment or practice might pose specific risk to workers with particular genetic variations; and
- it is the only reasonable method to obtain the required information.

If you are using genetic testing to obtain information for employment purposes, you should ensure that it is a valid method, which is subject to assured levels of accuracy and reliability. There should be scientific evidence that any genetic test is valid for the purpose for which it is used.

It's important to ensure that test results are carefully interpreted, taking into account how they might be affected by environmental conditions. You should also ensure that the results are always communicated to the worker tested and professional advice is available to them.

You should carry out a data protection impact assessment (DPIA) for any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the individual. However, a DPIA is required where this processing is combined with certain other criteria. For more detail see our separate guidance.

What about health monitoring?

In detail

What about the use of health monitoring technologies?

As an employer, you may decide to use health tracking technologies to help monitor the health of your workers. This might include workers using health and fitness tracking apps and wearables. These technologies may track things like a worker's heartbeat, their steps or other information, where the data is reported back to you or you have access to it. These may also involve the use of automated decision making or artificial intelligence.

When we refer to health monitoring technologies in this guidance, we mean devices that result in the collection and monitoring of information about workers' health, not just basic details that don't reveal the state of someone's health.

Examples

A warehouse worker is equipped with a wearable that tracks their physical activity for health and safety reasons.

A driver's company vehicle is fitted with a tachymeter to record miles and time logged to ensure they do not exceed safe limits on driving. The vehicle may be fitted with an in-cabin camera to measure driver tiredness (which may also involve the use of AI) to ensure they have appropriate rest stops and don't exceed legal limits on driving.

An office worker is asked to download a fitness app so their employer can monitor their activity levels to encourage wellbeing and to tackle issues with sedentary behaviour in an office environment (they may or may not receive some kind of reward or incentive if they use the app).

Employers may have an interest in ensuring the wellbeing of their workforce and may want to find ways to minimise staff absences resulting from ill-health. There may also be sector-specific or industry practices where an employer has specific duties and is required to monitor the health of its staff, for example, monitoring radiation exposure of workers in the nuclear industry. It is important to note that

this isn't limited to monitoring just physical health but can involve mental health and wellbeing.

This has become more noticeable as a result of the Covid-19 pandemic, with more generalised monitoring of workers' health. This included monitoring whether they may have been displaying Covid-19 symptoms or testing as positive cases, in an effort to reduce the spread of Covid-19.

The use of health monitoring technology goes beyond keeping a typical record of a worker's sickness and absence details and can have the potential to be much more intrusive. If you want to introduce health monitoring technologies, you need to be able to justify this as a proportionate and necessary measure to achieve your purpose. It also shouldn't be used in a way that is unfair or discriminatory to workers.

What do we need to consider if we want to monitor the health of workers?

You should first consider what you are trying to achieve and whether there is a less privacy intrusive way to do this. We recommend carrying out a data protection impact assessment (DPIA) before you start any processing. In some cases, you may be required to carry out a DPIA.

You also need to identify a lawful basis and a condition for processing special category data. Which lawful basis is appropriate will depend on your purpose(s) for the processing. Read our guidance on lawful basis for processing for more information.

You need to consider your other data protection obligations. For more information you should also read the section Data protection and worker health information which details the data protection issues you need to consider.

Can we ask workers to agree to the use of health monitoring technologies?

Consent as a lawful basis under data protection law is rarely appropriate in an employment setting given the imbalance of power between the employer and the worker. This is because it is difficult to demonstrate consent to be 'freely given' in these circumstances.

If you are required by law to actively monitor a worker's health, then consent would not be appropriate, and you should consider another lawful basis, such as legal obligation.

However, if you are offering a real choice for workers to participate in the use of health monitoring technologies, such as part of a worker wellness program, and

there is no risk of negative consequences for not doing so, then consent may be appropriate.

Remember, as health information is special category data, you also need a condition for processing. Explicit consent may be appropriate as your condition for processing. Please see the sections How do we lawfully process the health information of workers? and Can we rely on worker consent? for more information.

Example

An organisation wishes to offer its office staff the opportunity to participate in a wellbeing programme. One of the goals of this programme is to raise awareness of the health risks of inactivity and of sedentary behaviour.

The office workers are asked if they would like to take part and if so, to download a fitness app to monitor their activity levels during the day. Workers are offered a genuine choice whether to participate or not and can leave the programme at any time. They won't face any adverse consequences if they decline to participate, or later choose to leave the programme.

As participation is optional and there are no adverse consequences to those who do not want to take part the employer could consider consent as its Article 6 lawful basis. It could also consider explicit consent as its Article 9 condition for processing, making sure to properly record and document the worker's consent.

Further reading

Video surveillance

Data protection impact assessments

Guidance on AI and data protection

Explaining decisions made with AI

Rights related to automated decision making including profiling

Consent

When can we share worker health information?

In detail

Can we share health information of our workers?

There may be times when you need to share health information about your workers. Data protection law does not prevent you from sharing health information where it is appropriate to do so. However, these will be specific circumstances. This might be, for instance, as part of an occupational health referral or a legal claim, or under some other legal obligation. There may also be urgent or emergency situations in which you need to share information about a worker's health.

Whenever you want to share health information of workers you must:

- consider your purpose and ensure that it is reasonable and proportionate;
- treat your workers fairly and not use their health information in ways that would have unjustified adverse effects on them;
- tell workers about why and how you propose to share their health information before or at the time you share if this is not possible; and
- identify at least one lawful basis and a condition for processing before you start any sharing of health information.

You should also consider whether your ability to share health information is subject to other legal constraints outside of data protection law. For health information, this may include any duty of confidence that may apply, particularly where confidentiality is expected.

How do we ensure the lawfulness of sharing?

Before sharing any health information of a worker, you need to identify at least one lawful basis. You will also need a condition for processing. In order to comply with the accountability principle you must also be able to show that you considered this before sharing the information.

For most data sharing, it is better not to rely on consent as the lawful basis. If you cannot offer a genuine choice, consent is not appropriate. Employers are often in a position of power over workers and therefore should avoid relying on consent unless they are confident they can demonstrate it is freely given. Please see Can we rely on worker consent? for more information.

Remember, you need to meet your other data protection obligations, including fairness and transparency to ensure your data sharing is compliant.

Can we share worker health information in an emergency?

Yes. Data protection law allows organisations to share personal information in an urgent or emergency situation, including to help them prevent loss of life or serious physical, emotional or mental harm. In an emergency you should go ahead and share health information as is necessary and proportionate. Not every urgent situation is an emergency, but an emergency might include where there is the risk of serious harm to human life, such as preventing serious physical harm or loss of life.

Example

A worker is involved in an accident at work that seriously injurers them and renders them unconscious. An ambulance is called and paramedics arrive on the scene. The employer is aware that the worker has an underlying medical condition as part of a recent occupational health review, and informs paramedics to ensure that the worker receives appropriate care and treatment.

It is a good idea to plan ahead as far as possible for dealing with urgent or emergency situations. Having an emergency plan in place that takes into account data sharing can help prevent any delays in a crisis.

If you are likely to be involved in responding to emergency or critical situations (such as in high risk industries), you should consider in advance whether it is likely that you will need to share your workers' health information, in addition to other types of personal information. This might include information about a worker's mental health as well as their physical health, depending on the circumstances of the emergency. You should also consider how you will share the information securely. The best way to do this is through a data protection impact assessment.

You should factor in the risks involved in not sharing data, which could be more harmful than sharing data.

As part of your planning, you should ensure staff have clear guidance and training around their roles and responsibilities, to give them confidence in using and sharing personal information appropriately in an emergency situation.

Can we disclose information about a worker's health to other workers?

You should not normally need to share a worker's health information with other workers, beyond those who genuinely need the data to carry out their roles, for example your HR department.

Some job roles and industries may have legal requirements around an employer informing other staff about an individual worker's health condition. This is most likely to be for health and safety purposes, for example, where there is a high risk of a communicable disease that other workers may have been exposed to, or in areas with strict controls, such as food production. Where possible, you should avoid naming individual workers, but you can still let other people know that they may have been a close contact of a case.

If a worker has consented to your sharing their health information with other workers (perhaps they are on long-term sickness absence and want their colleagues to know the reason why), then it would be acceptable to share their information in such circumstances.

Further reading

Data sharing information hub

Data sharing Code

Lawful basis for processing

Lawful basis interactive guidance tool

Special category data

Accountability principle

Accountability Framework