

About this guidance	2
Data protection and workers' health information	4
How do we handle sickness and injury records?	24
What if we use occupational health schemes?	29
What if we use medical examinations and drugs and alcohol testing?	33
What if we use genetic testing?	43
What if we carry out health monitoring?	45
When can we share workers' health information?	49
Checklists	53

# About this guidance

■ [Latest updates - last updated 31 August 2023](#)

**31 August 2023** - This guidance was published.

## In detail

- [Who is this guidance for?](#)
- [How is this guidance structured?](#)
- [What do you mean by 'worker'?](#)
- [How should we use this guidance?](#)

### Who is this guidance for?

This guidance is aimed at employers to help them understand their data protection obligations under the UK GDPR and DPA 2018 (we refer to these as 'data protection law') when handling the health information of the people who work for them. The guidance also provides links to other pieces of key data protection guidance if you want to find out more information.

The guidance aims to:

- help provide greater regulatory certainty;
- protect workers' data protection rights; and
- help employers to build trust with workers.

### How is this guidance structured?

The guidance has two main parts. The first section contains an overview of how data protection law applies to the processing of workers' health information. It looks at the data protection principles and the basics for compliance, with links to further detailed guidance.

The second part considers some of the most common types of employment practices where you process workers' health information. It looks at what the law requires you to do, as well as good practice advice.

While we recommend that you read the guidance in full, you can choose which parts of the guidance you read to fit your needs.

### What do you mean by 'worker'?

We use the term 'worker' throughout this guidance only to refer to someone who performs work for an organisation. Business models have changed in the last decade, with the rise of the gig economy. This guidance captures these relationships too. It is aimed at all circumstances where there is an employment relationship or otherwise a relationship between an organisation and a person who performs work for the

organisation, regardless of the nature of the contract.

## How should we use this guidance?

To help you to understand the law and good practice as clearly as possible, this guidance says what organisations **must**, **should** and **could** do to comply.

### Legislative requirements

- **Must** refers to legislative requirements.

### Good practice

- **Should** does not refer to a legislative requirement, but what we expect you to do to comply effectively with the law. You should do this unless there is a good reason not to. If you choose to take a different approach, you must be able to demonstrate that this approach also complies with the law.
- **Could** refers to an option or example that you could consider to help you to comply effectively. There are likely to be various other ways you could comply.

This approach only applies where indicated in our guidance. We will update other guidance in due course.

# Data protection and workers' health information

## In detail

- Why is it important that the health information we have on workers complies with data protection law?
- How do we ensure we use workers' health information fairly?
- How do we lawfully process workers' health information?
- What lawful bases might apply if we want to process workers' health information?
- What special category conditions might apply?
- Can we rely on a worker's consent?
- How do we limit how much health information we collect?
- What do we need to tell workers when processing their health information?
- How long can we keep workers' health information?
- How do we keep workers' health information accurate and up to date?
- How do we keep the health information of workers secure?
- What if we use automated decision making involving workers' health information?
- Do we need to do a data protection impact assessment?
- Who is responsible for data protection and health information in our organisation?
- Checklist

## Why is it important that the health information we have on workers complies with data protection law?

Health information is some of the most sensitive personal information you might process about your workers. The UK GDPR and the DPA 2018 (referred to here as data protection law) applies whenever you process information about your workers' health.

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, but is not limited to:

- a questionnaire completed by workers to detect problems with their health;
- sickness absence forms;
- information about their impairment or disability;
- the results of a worker's eye-test who has been 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 personal information, including 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 information 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 you can do it.

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

### Further reading

You can read our [separate detailed guidance on special category data](#), which includes further information on '[What is health data?](#)'. It also covers '[What about inferences and educated guesses?](#)'. This considers whether inferences about people can count as special category data, which may be relevant to your use of health information.

## How do we ensure we use workers' health information fairly?

If you want to collect and use information on your workers' health, you **must** be clear about why you are doing so. You **must** also have justifiable 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.

Remember that gathering information about your workers' health is intrusive and in some cases it may be highly intrusive, depending on the sensitivity of the information. It is though reasonable for workers to expect they will need to share a proportionate amount of health information with you, for example when dealing with:

- sickness absence;
- occupational health referrals; and
- other employment-related purposes.

However, workers can legitimately expect that employers will respect their privacy when handling their health information.

Data protection law requires fairness. In general, you **should** 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 and transparent about your purposes for processing health information from the start. You **should** carefully consider not only how you can use their health information, but also the reasons why you need to use their information.

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

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.

Remember to consider your obligations under employment law, health and safety law and other legislation. Remember to also consider any common law duties, as well as any relevant industry standards you may have.

### Further reading

Read our guidance on:

- [Lawfulness, fairness and transparency](#)
- [Special category data](#)
- [Purpose limitation](#)

## How do we lawfully process workers' health information?

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. You cannot process this type of information unless you meet some additional requirements. This means that, in addition to a lawful basis, you **must** also identify a special category condition for processing under Article 9 of the UK GDPR. You may also need to satisfy a condition in schedule 1 of the DPA 2018. For more information on this, see '[What special category conditions might apply?](#)' below.

Lawfulness also means that you don't do anything with workers' health information which is unlawful in a general sense (eg statute and common law obligations, whether criminal or civil). If your processing of health information involves committing a criminal offence, it will obviously be unlawful. However, processing may also be unlawful if it results in:

- a breach of a duty of confidence;
- a breach of industry-specific legislation or regulations; or
- a breach of the Human Rights Act 1998.

These are just examples and this list is not exhaustive. You may need to take your own legal advice on

other relevant legal requirements.

Below, [we set out the lawful bases that are most likely to apply in an employment context](#) when you need to process your workers' health information.

### Further reading

You can use our [interactive guidance tool](#) to help you decide which lawful basis might apply.

You can find more information about the following:

- [Lawfulness, fairness and transparency](#)
- [Lawful basis for processing](#)
- [Special category data](#).

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

There are six lawful bases for processing personal information. At least one of these **must** apply whenever you process health information. No one basis is better, safer or more important than the others. How you decide which lawful basis applies depends on your specific purposes and the context of the processing of workers' health information. Remember, you **must** determine your lawful basis for processing your workers' health information before you begin this processing. You **must** document it.

We've listed below the lawful bases that are most likely to apply to the processing of workers' health information in an employment context. Other lawful bases may be available.

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 it's likely you can rely on it.

### 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. This lawful basis only applies to processing purely for contractual employment purposes, rather than legal obligations under employment law.

## Example

As part of their contract of employment with their workers, an employer provides occupational sick pay. This is a type of contractual sick pay and is distinct to statutory sick pay, which is a legal requirement. The employer needs to process details of their workers' sickness absences to pay occupational sick pay. They therefore rely on contract as their lawful basis. They also identify a special category condition for processing the health information.

## Further reading

[Contract](#)

## Legal obligation

You can rely on this lawful basis where you need to process a worker's health information to comply with the law (although this does not include contractual obligations).

## Example

An employer has a legal requirement to report 'specified injuries' to the Health and Safety Executive, under RIDDOR 2013. This would involve the processing of a worker's health information. The employer relies on legal obligation for their lawful basis. They also identify a special category condition.

## Example

An employer needs to process sickness absence information about their workers in order to comply with their legal obligation to pay statutory sick pay. The employer therefore relies on legal obligation as their lawful basis.

The employer also identifies an appropriate special category condition.

## Further reading

[Legal obligation](#)



## 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. As part of this, you **should** carry out a legitimate interests assessment to determine if this is the case.

### Example

An employer is being sued by one of their workers following an accident at work. The employer wants to share details of the accident with their solicitors to obtain legal advice on their 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 employer carries out a legitimate interest assessment and they are satisfied they can rely on legitimate interests in sharing the health information. They also identify a special category condition for processing.

### Example

An employer needs to recruit for a position where the health and fitness of the post holder is integral to the role. Therefore, they want to ensure that the person they employ passes a health exam. They decide to make their job offer conditional on the shortlisted person subsequently having a medical exam prior to starting employment. As a result, they need to collect this person's health information.

The employer determines that it is in their legitimate business interests to have fully vetted staff, given the nature of the work. They consider the different job roles and determine that the level of vetting depends on the type of role. They assess what checks and vetting are actually necessary for each role. This ensures that the processing is targeted and proportionate to the specific role and responsibilities in order to meet the necessity test. For their lawful basis, the employer relies on legitimate interests. They also identify a special category condition for processing.

### Further reading

For further information see our guidance on [Legitimate interests](#) and in particular the see the section '[How can we apply legitimate interests in practice?](#)'.

## Vital interests

In exceptional circumstances, you may be able to rely on the vital interests lawful basis if you need to process a worker's health information to protect their life, or the life of another person. You cannot rely on vital interests for health information if the worker is capable of giving consent, even if they refuse their

consent. This lawful basis is very limited in its scope and generally only applies to matters of life and death. For example, this lawful basis may apply where there is a medical emergency and a worker's life is at immediate risk.

### Further reading

[Vital interests](#)

## What special category conditions might apply?

As explained above, health information is special category data. This means that as well as identifying a lawful basis under Article 6, you **must** also identify a special category condition under Article 9. There are 10 conditions for processing special category data. For five of these conditions, you **must** meet additional conditions and safeguards set out in schedule 1 of the DPA 2018.

If you are relying on a schedule 1 condition, 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.

### Further reading

See our separate guidance '[What is an appropriate policy document?](#)' for more information. We have also produced a [template](#) you can use.

See also [Special category data](#).

Remember that you **must** determine your special category condition before you begin the processing. You **must** document your decision, along with your lawful basis.

We've listed below the most likely special category conditions relevant to processing workers' health information in an employment context.

## Employment, social security and social protection law

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

- ensuring the 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 identify the legal obligation or right in question, either by reference to the specific legal provision or 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. In the context of workers' health information, this would be a legal obligation or right that requires you to process their health information.

This condition does not cover processing to meet purely contractual employment rights or obligations (such as occupational sick pay, which is given above as an example of processing based on the contract lawful basis. However, processing for the purpose of paying statutory sick pay would be covered by the condition).

You **must** justify why processing 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 special category condition, you also **must** meet the associated condition set out in part 1 of schedule 1 of the DPA 2018. This condition also means you **must** have an appropriate policy document in place.

### Further reading

[Employment, social security and social protection law](#)

## Legal claims or judicial acts

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

### Example

An employer is being sued by one of their workers following an accident at work. The employer wants to pass the details of the accident to their solicitors to obtain legal advice on their 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.

The employer has also identified a lawful basis, such as legitimate interests (see above).

You **must** justify why processing 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.

### Further reading

[Legal claims and judicial acts](#)

## 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 on this condition, you **must** 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.

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

- statutory and government purposes; and
- safeguarding of children and of individuals at risk.

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

### Further reading

Read our guidance on:

[Substantial public interest](#)

For more information on the different conditions see:

[Substantial public interest conditions](#)

## Other resources

[Schedule 1, Part 2 of the Data Protection Act 2018](#)

External link

## Vital interests

You may also find that vital interests might apply in some limited circumstances, similar to the vital interests lawful basis as discussed above.

### Further reading

[Vital interests](#)

## Can we rely on a worker's consent?

Here, we consider the issue of relying on a worker's consent as a lawful basis or explicit consent as a special category condition. This is because consent provides certain challenges in an employment context.

Consent is one of the lawful bases for processing personal information. Data protection law 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). You **must** also allow people to withdraw their consent as easily as they give it.

However, you may find it difficult to rely on consent to process health information 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, they cannot freely give their consent. If the worker has no genuine choice over how you use their information, you cannot rely on consent as a lawful basis.

### Example

A company requires their workers wear a device to monitor their movements for time management and complex stock movement purposes. The company considered whether less intrusive methods would meet these purposes but decided these alternative methods do not meet their business needs.

The wearable device also has the ability to monitor heart rate. The company asks their workers to consent to the additional collection of heart rate information to measure their fitness levels in order to contribute to performance evaluation purposes. 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 come across as difficult or having something to hide.

As the workers' consent is not freely given, the company cannot rely on consent or explicit consent in this example. This is because of 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 refuse without fear of a penalty being imposed. They **must** also be able to withdraw their consent at any time.

If you think it will be difficult for you to show that your workers' consent is freely given, you **should** consider relying on a different lawful basis, such as legitimate interests. See '[What lawful bases might apply if we want to process workers' health information?](#)' for other lawful bases that you may consider using for the type of processing you want to do.

However, this does not mean that 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 workers have freely given their consent.

### Example

A medical firm offers health screening for their staff, using their own in-house services to test and examine their workers. The firm makes it clear that there is no requirement to take part. They say that

they will not take participation into account for performance evaluation purposes or any purpose other than the voluntary health screening.

Participation is genuinely optional and there are no adverse consequences to those who do not want to take part. Therefore, the firm can consider consent as their lawful basis. They can also consider explicit consent as their special category condition for processing.

There are also other considerations you **must** take into account if you want to rely on consent, such as recording and managing consent.

## Explicit consent

Explicit consent is one of the conditions that you can use to process special category data, including health information. Data protection law does not define explicit consent. However, it is not likely to differ much from the usual high standard of consent. The key difference is that a person **must** expressly confirm their explicit consent in a clear statement (whether oral or written). You cannot infer explicit consent from someone's actions.

Explicit consent is the only special category 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.

### Further reading

For more information please see our [separate guidance on consent](#) and on [explicit consent](#).

## 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. The information you do collect **must** be relevant and adequate to properly fulfil that purpose.

You **should** consider whether there are 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 **could**, if appropriate to meet your business needs and the role's physical requirements, use a health questionnaire to select the people you are testing.

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 depends on what is necessary for certain job roles. Some roles 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 at risk people.

This will often be for health and safety reasons. You **should only** collect more detailed health information in areas of highest risk.

### **Example**

An employer decides to use a health questionnaire for their workers to ensure they are medically fit to work in a physical job role. The employer ensures that they only collect information that they really need. They design the health questionnaire to ensure it only collects relevant information.

It is good practice for health professionals to design health questionnaires. This also means the questionnaires **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 your legal obligations.

### **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 details of the worker's condition. They ask the author to provide an assessment of whether or not the worker is fit to return to employment, whether they need to be redeployed or whether the employer needs to make adjustments 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 the employer needs information from a GP or other medical professional, they ask the worker specific, relevant questions to elicit the information needed.

Where an employer needs to obtain a report from a worker's GP or other medical practitioner responsible for the worker's care, the employer considers 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 you may find it useful in the future.

However, you may 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 their workers who do hazardous construction work. The employer has safety procedures in place to help prevent accidents. Therefore, the employer may never need this information, but they still need to hold this information in case of an emergency.

However, it may be excessive to hold details of the blood groups of the rest of the workforce who aren't involved in hazardous work, such as office staff.

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, leave it to medical professionals to access and interpret detailed medical information for you. See also '[What if we use occupational health schemes?](#)' and '[What if we use medical examinations and drugs and alcohol testing?](#)'.

Remember that workers have a right to rectification and a right to erasure about their personal information.

### Further reading

For more information see our separate guidance on [data minimisation](#).

You can also read our separate guidance on the [right to rectification](#) and the [right to erasure](#).

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

Data protection law requires fairness and transparency. It provides a right for workers to be informed about how their employer is using their health information 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 your workers 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 you might collect health information or share it with others;



- as a general notice on a staff notice board; or
- by sending a letter or email to workers.

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

Where you are taking a specific action, for example if a worker is undergoing a medical test, you **must** ensure, prior to the test, that the worker is fully aware what, why and how much information you are collecting. They also need to know 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 if we use occupational health schemes?](#)' and '[What if we use medical examinations and drugs and alcohol testing?](#)'.

### Further reading

Read our separate 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 workers.

For more on data protection rights see:

[Individual rights](#)

## How long can 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. You also need to justify keeping this information. This depends on your purposes for holding the information.

Where you are processing health information, you **must** record your retention schedules to comply with documentation requirements. 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 and health and safety records.

Remember to consider any legal or regulatory requirements and seek advice on compliance if necessary. There are various legal requirements and professional guidelines about keeping certain kinds of records,

such as information on aspects of health and safety. Certain legislation may require you to keep the information for a specified period. This might mean you need to keep health information to comply with such a requirement.

You also **must** 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 you collected it.

This principle closely links to the data minimisation principle. For more details, see '[How do we limit how much health information we collect?](#)' above.

### Further reading

For more information on how long you can keep personal information please read our [separate guidance on storage limitation](#).

See also our [separate guidance on Documentation requirements](#).

We also have [separate guidance on the right to erasure](#).

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

Data protection law requires you to ensure personal information is accurate and, where necessary, kept up to date (the accuracy principle). You **must** take all reasonable steps to ensure your workers' health information is not incorrect or misleading as to any matter of fact.

You **must** 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 information about a worker's blood type, the information 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, you may need to update these. It is probably worth asking the worker concerned to review and confirm any changes.

If you discover that the 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 by your workers to the accuracy of their health information.

If your workers have the ability to input or update their own health information on your organisation's system (such as your HR platform), your ability to ensure accuracy of the information may be more limited. However, you **could** carry out periodic reviews of your workers' records. If you decide to review worker records, you **should** ensure that appropriately authorised people carry out this work. You may prefer to instead ask workers themselves to periodically check the information they enter.

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

### Further reading

Read our separate guidance on:

- [Accuracy](#)

- [Right to rectification](#)
- [Right to erasure](#)

## How do we keep workers' health information secure?

Data protection law requires that you **must** have appropriate security measures in place to protect your workers' health information. This is the 'integrity and confidentiality' principle – also known as the security principle.

You **must** ensure the level of security you apply is appropriate to the nature of the information you are protecting and harm that might result from misuse or loss. Given that health information is special category data, you **must** have a high level of security. Unless you apply a particularly high level of security to all employment records, it is likely that you would need to single out health information about your workers for special treatment. This means you **must** keep information about workers' health particularly secure.

Depending on the nature of your organisation, you **could** keep information about your workers' health on a separate database or system, or subject to separate access controls. For example, limiting access to only those who need to see it, such as using password protection. If you use physical records, you **could** separate health information from the other contents of a worker's personnel file (such as by putting it in a sealed envelope) and keeping it in a locked cabinet.

You **should** also consider who has access to workers' health information. You **should** apply the principle of 'need to know'. As far as possible, you **should** limit access to information on medical conditions to health professionals, such as doctors and nurses.

Managers **should only** have access where it is necessary for them to undertake their management responsibilities. You **should** limit this to only the information they need to meet their obligations. It's likely you can limit this to information about a worker's current or likely future fitness to work. It may be less information than a doctor or nurse needs 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 developing your information management systems, you **must** consider data protection by design and by default. This ensures that data protection is built into your systems. If you are reviewing your existing systems, you **must** consider how you can incorporate this requirement.

### Further reading

We have produced [separate guidance on security](#).

Read our separate guidance on [data protection by design and by default](#).

## What if we use automated decision making involving workers' health information?

You may sometimes want to use automated decision-making about your 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, you might use profiling to analyse or predict aspects of a worker's performance.

Article 22 of the UK GDPR stops 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 can meet one of these, there are additional requirements you **must** satisfy. These include allowing workers to request human intervention or to challenge a decision. As this kind of processing is considered high-risk in terms of the potential impacts on people, you **must** carry out a data protection impact assessment (see '[Do we need to do a data protection impact assessment?](#)' below).

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 data protection principles and identify and record your lawful basis and special category condition for the processing of health information.

You **must** have processes in place so workers can exercise their rights.

People have a right to object to profiling in certain circumstances. You **must** bring details of this right specifically to the attention of your workers.

### Further reading

We have produced separate guidance on [artificial intelligence and data protection](#), which includes a section on [the application of Article 22 where automated decision making involves the use of artificial intelligence](#).

See also:

- [Rights related to automated decision making including profiling](#)
- [Automated decision-making and profiling](#)

## Do we need to do a data protection impact assessment?

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 workers and your organisation.

Under data protection law you **must** 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.

You **should** carry out a DPIA given the sensitive and potentially intrusive nature of processing workers'

health information. As noted above, it may be a requirement depending on the processing you want to do. A DPIA also provides you with the opportunity to involve your workers before you start any new processing of their health information.

Throughout this guidance, we highlight issues we recommend you **should** consider 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 a general overview, read our [separate guidance on data protection impact assessments](#).

For further information, read our [detailed DPIA guidance](#).

The following sections may also be particularly useful:

- [When do we need to do a DPIA?](#)
- [What does the ICO consider likely to result in high risk?](#)
- [Do we need to consult the ICO?](#)

We have also produced a [DPIA template](#) that you can use.

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

Accountability is one of the key principles in data protection law. The accountability principle means that you **must** take responsibility for what you do with health information and how you comply with the other principles.

You **must** have appropriate measures and records in place to demonstrate your compliance with your data protection obligations. This doesn't just include compliance with the principles (as explained in the preceding sections). It also includes 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 health information that are likely to result in high risk.

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.

### Further reading

For more information, see our separate guidance on:

- [Accountability principle](#)
- [Accountability and governance](#)
- [Data protection by design and default](#)
- [Documentation](#)
- [Data protection impact assessments](#)

We have also 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.

Ultimately, your organisation, as the controller, has responsibility for data protection compliance. If you use any processors that are processing health information on your behalf, you **must** ensure you have a written contract in place with them.

#### Further reading

See our separate guidance on [controllers and processors](#) and also on [contracts](#) for more information.

If you have a data protection officer, you **must** involve them in any decisions about your processing of health information.

#### Further reading

[Data protection officers](#)

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

#### Further reading

For more information, read our [separate guidance on individual rights](#).

## Checklist: Data protection and workers' health information

We have checked the processing of health information is necessary for the purpose we have

identified and are satisfied there is no other reasonable and less intrusive way to achieve that purpose.

- We have identified a lawful basis for processing the health information.
- We have identified a special category condition for processing the health information.
- We avoid overly relying on consent when processing workers' health information unless we can demonstrate it is genuine and freely given
- We have documented what health information we are processing.
- Where required, we have an appropriate policy document in place.
- We have considered whether we need to do a data protection impact assessment.
- We ensure we only collect and use health information that is adequate, relevant and necessary and do not hold more than we need for the purpose.
- We included specific information about our processing of health information in our privacy information for workers.
- We have considered our retention policy on health information and keep the health information of workers only for as long as necessary.
- We ensure we keep the health information of our workers accurate, and where necessary, up to date.
- We put in place appropriate security measures to protection the health information of our workers.
- If we use health information of workers for automated decision making (including profiling), we have checked we comply with Article 22.
- We have considered how the use of the health information of our workers affects our other obligations such as accountability, data protection by design and default, and appointing Data Protection Officers (DPOs).
- We understand our obligations when workers exercise their data protection rights.

[You can also view and print off this checklist and all the checklists of this guidance on our checklists page.](#)

# How do we handle sickness and injury records?

## In detail

- [What are sickness, injury and absence records?](#)
- [Can we process sickness and injury records?](#)
- [How do we lawfully process sickness and injury records?](#)
- [How do we store sickness and injury records?](#)
- [How do we limit access to sickness, injury and absence records of individual workers?](#)
- [Can we share information from sickness or injury records?](#)
- [Checklist](#)

## What are 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.

For the purposes of this guidance only, we distinguish between sickness, injury and absence records in the following ways:

- **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. You **could**, and you may prefer, to use absence records instead of sickness records where practical. These are generally less intrusive to workers' privacy. A simple absence record, without any details of a worker's health condition is not likely to be special category data.

See also '[How do 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 you to review your workers' ability to undertake their work. They are necessary for other purposes, such as identifying health and safety hazards at work and for paying health-related benefits to workers.



However, you **should** make sure that you do not use sickness and injury records 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. You also need to consider whether full access to the record 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 inappropriate use of sickness records. This would not fall within someone's reasonable expectations of how an employer may handle their sickness information.

An employer **must not** publish 'league tables' of sickness absences of individual workers 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, the employer **could** publish totals of sickness absence by department or section, as long as individual workers are not identifiable.

You **should** 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. Holding sickness or injury records therefore involves processing 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 legal obligations, including:

- under employment and health and safety law;
- to meet 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.

It's unlikely that consent as a lawful basis and explicit consent as a condition for processing would ever be appropriate as a basis for processing sickness records. This is because a worker is unlikely to have the ability 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 do 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 staff are not accessing information on a worker's health when they only need information on absence or the circumstances of an accident at work.

See '[How do we limit access to sickness, injury and absence records of individual workers?](#)' below for more information.

It is a good idea to review how you currently keep your sickness and accident records. If necessary, you **should** change the way you keep information on sickness and accidents.

You **must** ensure you take appropriate measures to keep sickness and injury records secure, especially given the sensitive nature of the information. You **could** do this by keeping the sickness record in a specially protected computer file, perhaps using encryption. If you use physical records, you **could** keep it in a sealed envelope, stored in a locked filing cabinet.

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

You **should not** make the sickness, injury or absence records of individual workers available to others, 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, a manager can access a worker's sickness record 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 how to handle them appropriately.

How much personal information from sickness records people in your organisation can access depends on the purpose of your processing.

You **should** make it clear to those accessing sickness, injury and absence records 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 a worker's health condition and the reasonable adjustments they need because of their health condition. This enables the organisation to keep a record of the worker's agreed adjustments. If the worker moves to a different team, their new manager can access this 'passport'.

The organisation needs to inform their facilities team of the reasonable adjustments necessary to the worker's workstation. The facilities team can 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 you only need information about the length of an absence. Similarly, you **should not** use sickness records for a particular purpose when you can use records of absence instead. For example, you do not need to use a sickness record when you only need information on absence or the circumstances of an accident at work.

### Example

When an employer is calculating a benefit, admin staff may only need to see the length of a worker's absence, rather than details 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 it is necessary and proportionate to do so. This might include 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.

This is not an exhaustive list. There may be other situations that you can justify.

You **should** 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. It's also important to point out that this doesn't prevent you from sharing information from a worker's sickness or injury record if the information is relevant to you responding to a medical emergency.

See '[When can we share workers' health information?](#)' for more information. This also addresses circumstances involving disclosing information about a worker's health to other workers.

## Checklist

- We distinguish between sickness, injury, and absence records.
- Where we only need to know information about the length of a worker's absence, and where practical, we consider using absence records instead of sickness records.
- We limit who can access and use information about workers from sickness and injury records, including whether they can have full access to the information of workers. We ensure they know what they can and cannot do with the health information.

- We only use sickness and injury records in ways that workers would reasonably expect.
- We have identified a lawful basis and a special category condition for processing sickness and injury records.
- We only share information from sickness or injury records about a worker's illness, medical condition or injury with third parties where it is necessary and proportionate to do so. For example:
  - there is a legal obligation;
  - it is necessary for legal proceedings; or
  - the worker has given explicit consent to the sharing.

[You can also view and print off this checklist and all the checklists of this guidance on our checklists page.](#)

# What if we use occupational health schemes?

## In detail

- [What does this section cover?](#)
- [What do we tell workers when using an occupational health scheme?](#)
- [Are occupational health providers controllers or processors?](#)
- [What do we need to do when requesting a worker's medical file as part of an occupational health referral?](#)
- [How do we ensure we respect workers' confidential communications with health professionals?](#)
- [How do we limit who has access to medical information about workers?](#)
- [Checklist](#)

## What does this section cover?

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

## What do 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. You **must** make this clear from the outset, as part of your transparency obligations. This includes when you may share their information with external occupational health providers and what information you may get back from them. You can read ['What do we need to tell workers when processing their health information?'](#) for more information on this.

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

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](#)
- [Individual rights](#)

## Are occupational health providers controllers or processors?

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

### Example

Company A contracts the occupational health provision for their workers to Company B. Company B is a professional occupational health provider and their staff comply with their own medical obligations. Company B determines the purposes of the processing of Company A's workers' health information. Company B is the controller when processing the information of workers referred to them for their occupational health service.

This also means that the occupational health provider **must** comply with their 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 you are the controller for any personal information about your workers that you obtain for your own purposes from the occupational health provider.

You **must** 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.

### Further reading

- [Controllers and processors](#)
- [Contracts](#)
- [Individual rights](#)
- [Data sharing agreements](#)

## 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](#)

### Other resources

- [Access to Medical Reports Act 1988](#) ↗
- [Access to Health Records \(Northern Ireland\) Order 1993](#) ↗

## How do we ensure we respect workers' confidential communications with health professionals?

You **should 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 you set your systems up in such a way that you unintentionally pick up a confidential conversation or other communication, you **should** delete information about that conversation or communication at the earliest opportunity. You **should not** keep any record of it.

You may find it 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' or 'private' to help you avoid reading confidential messages.

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




You **should** only make medical details about workers available to managers where necessary to allow them to discharge their management responsibilities. You **should** keep this type of access to a minimum. As far as possible, an occupational health advisor **should** hold the medical information about a worker and only tell the worker's manager the results of the health assessment. For example, they can explain 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. They might need to have some access to that worker's health information, particularly if the worker needs changes to their workplace as a result. The key point is that you **should** ensure only information that is genuinely needed for those to carry out their roles effectively is available to them.

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 need to obtain explicit consent for the release of such information to non-medical staff.

Consider whether you need to comply with any guidance from relevant professional bodies and regulators, such as the General Medical Council (GMC) or Health and Care Professions Council.

### Other resources

- [General Medical Council](#) 
- [Health and Care Professions Council](#) 
- [Faculty of Occupational Medicine](#) 

## Checklist

- We tell our workers how we intend to use information they provide as part of an occupational health scheme and the reports produced as a result. We also tell them who it might be made available to and why.
- We tell workers what data protection rights they have around the use of their information.
- We consider implementing a data sharing agreement with the occupational health provider, setting out under what terms information will be shared.
- We ensure that when requesting a worker's medical file as part of an occupational health referral, we handle any information received in accordance with data protection law.
- We don't ask workers to consent to the disclosure of their entire medical record, unless this is absolutely necessary.
- We avoid compromising any confidential communications between workers and health professionals in an occupational health service.

[You can also view and print off this checklist and all the checklists of this guidance on our checklists page.](#)



# What if we use medical examinations and drugs and alcohol testing?

## In detail

- [What does this section cover?](#)
- [Why might we want to obtain information from medical examinations and drugs and alcohol testing?](#)
- [What do we need to consider if we want to introduce medical examinations and testing?](#)
- [Can we use medical examinations and testing as part of our recruitment process?](#)
- [How do we limit the purpose of the examination or testing and the information we obtain?](#)
- [What do we tell workers about examinations and testing?](#)
- [Can we retain information obtained from medical examination or testing?](#)
- [How do we ensure drugs and alcohol testing is appropriate?](#)
- [How much personal information can we collect from drugs and alcohol testing?](#)
- [How do we select workers for drugs and alcohol testing?](#)
- [Can we use random testing?](#)
- [How do we ensure testing is of a good standard and quality?](#)
- [Checklist](#)

## What does this section cover?

This section of the guidance considers your data protection responsibilities when you want to collect health information about your workers. This covers both medical examinations and medical testing, such as for drugs and alcohol use. Many of the considerations are the same, whether you are collecting information from medical exams or from testing of workers. However, where these are different, we highlight specific issues for you to take into account.

This guidance does not address consent for any physical intervention involved in taking a sample from a worker in the course of medical testing.

## Why might we want to obtain information from medical examinations and drugs and alcohol 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). You 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?](#)' below.

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

- prevent a significant risk to the worker’s health and safety 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 they might return;
- 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 at 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 provide an optional occupational health and wellbeing programme, for example to promote physical and mental health and wellbeing. This may include an element of testing workers’ health. However, this **should only** take place where workers have a free choice to participate. You **must** clearly explain to them how you might use their personal information and the potential consequences of taking part.

Workers employed on overseas contracts may need 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. Certain countries may also have a legal requirement for medical testing. You **must** make sure that you are transparent with workers about any examination or testing that they need to undergo at an early stage.

## What do we need to consider if we want to introduce medical examinations and testing?

You **must** record the purpose of your proposed programme of examination or testing of workers. You **must** identify your lawful basis and special category condition for processing. You may wish to do this as part of your data protection impact assessment (DPIA).

You **should** also document:

- who you are going to test or examine;
- what precisely you are testing or examining them for;
- the frequency of testing or examinations; and
- the consequences of a positive or negative test or the result of an examination.

You **should** consider whether there are any less intrusive ways of meeting your objectives as an employer, unless you are legally required to carry out a test or examination. This might mean, for example, collecting information via a health questionnaire either as a first stage or as an alternative to a medical examination, if this is appropriate given the nature of the role.

### Further reading

[Data protection impact assessments](#)

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

Medical examination and testing are, even if needed for the role, inherently intrusive. You **should only** use them to obtain information where this is necessary to meet your purposes. This means employers **should not** by default submit all job applicants, or even those shortlisted, to medical 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, in many cases, going to be where there is a likelihood of appointing them subject to satisfactory examination or test results.

You **should** also satisfy yourself 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 **must** record your purpose for introducing the examination or testing and your lawful basis and special category 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 need to undergo medical examination or testing if you are likely to appoint them.

Decisions on a worker's suitability to work are management decisions. However, you **should** leave the interpretation of medical information to a suitably qualified health professional.

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

You **must** be clear from the outset about why you are carrying out the testing or examination, including what substances or conditions you are looking for. You **should** 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.

You **should** design the testing or examination 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 you have not told the worker about and that they have 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 test a worker's blood sample for the presence of alcohol when they were only told it was being testing it for the presence of a particular chemical which the worker might have been exposed. The employer would not be complying with data protection law in this case.

## Further reading

[Purpose limitation](#)

## What do we tell workers about examinations and testing?

You **must** ensure that workers are fully aware when testing is taking place or where you require medical examinations, 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 you may discipline them when being tested for alcohol; and
- the possible consequences if they breach the policy.

You **could** 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. It would be deceptive and misleading to workers if you attempted to obtain information by collecting samples covertly, or by testing existing samples in a manner that you had not told workers 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. You are unlikely to ever justify covert medical testing 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 you clearly set these out to your workers. 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 **should** explain similar considerations if you want your workers to undergo medical examinations, or the law requires them to do so.

## Can we retain information obtained from medical examination or testing?

You **must** permanently delete information obtained from medical examination or testing that is not relevant for your purpose(s).

### Example

A worker is drug tested for a particular substance. The information obtained during the drug test indicates the presence of another substance. The worker is in fact taking prescribed medication to treat a condition the employer is not aware of. The medical condition is minor and has no bearing or impact on the worker's ability to carry out their role. The employer **should not** record or use the information. In addition, the employer **should** ensure it designs the test, 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 (for example where necessary for the operation of an occupational health service), you **must** keep it securely and confidentially in an appropriate storage system.

## How do we ensure drugs and alcohol testing is appropriate?

You **should** make sure that the information you collect from drugs and alcohol testing is designed to ensure safety at work rather than just to reveal the illegal use of substances in a worker's private life. For example, you may need to employ testing due to the nature of a worker's role, such as pilots, drivers or machine operators where they make safety-critical decisions. In other roles, you may not need to conduct testing. Instead, you may be able to handle performance or behavioural issues potentially related to drug or alcohol usage through staff conduct policies rather than through testing.

This is because testing workers for drugs or alcohol is intrusive and very few employers can justify 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 **should** 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 **should not** test merely to find evidence of the use of illegal drugs.
- The drug testing you use **should** address the risk. You **should** ensure the testing is 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, you are unlikely to justify regular drug testing unless there is a reasonable suspicion of drug use that has an impact on safety.
- Consider whether drug testing provides 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 can we collect from drugs and alcohol testing?

You **must** minimise the amount of personal information you obtain from testing for the presence of drugs and alcohol in your workers.

You **should** use drug or alcohol testing only 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. In some cases, such as in illegal drug consumption and alcohol consumption, effects are well documented and this will be straightforward. 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 **could** 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. If you intend to carry out testing you **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 you can use 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 drugs and alcohol testing?

When you select workers for drugs and alcohol testing, you **must** ensure that you justify, properly document, adhere to and communicate to workers the criteria you use.

## 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. You record the decision that the worker is required to undergo a drugs and alcohol test. You also record the results of the test.

## Can we use random testing?

You cannot justify collecting personal information by testing all workers in your organisation 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, you can rarely justify collecting information through the random testing of all workers.

## Example

At a rail company, 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 a ticket inspector or rail enquiries clerk. The employer **should** reflect this difference in risk in their DPIA. They **should not** test ticket inspectors or rail enquiries clerks simply on the basis that fairness somehow requires that if drivers or signal engineers are tested, they need to be tested as well.

It is generally unfair and deceptive to lead workers to believe that you are carrying out random testing if, in fact, you are using other criteria. If you are using other criteria to trigger testing, you **must** ensure workers are aware of your true testing criteria.

If you do carry out random testing, you **should** ensure that you carry it out in a genuinely random way.

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

It is important you ensure that any health information you obtain through testing is:

- of sufficient technical quality to support any decisions or opinions that you derive 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.

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. This is because the reliable interpretation of test results can require a high level of technical expertise. However, you don't need to employ health professionals to undertake tests for alcohol using breath analysis equipment.

Although sample kits that employers can use 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.

## Checklists

### **Deciding when to collect information through medical examinations and testing**

- We are able to justify collecting information through medical examination and testing of workers.
- We have made it clear to workers the rules and standards and when we may use tests to help enforce these.
- We carry out a data protection impact assessment to help document our purposes, justifications, safeguards, and how we intend to comply with our data protection obligations.
- We consider other less intrusive means of achieving our purposes, such as a health questionnaire instead of testing.

### **Carrying out medical examinations and testing**

- We tell workers what they are being tested for, the frequency of testing, and the consequences of the results.
- We use the least intrusive forms of medical examination and testing that will bring the intended benefits to our organisation.
- We ensure that the testing method is of good quality, reliable and provides accurate results.
- We only collect information if it is a necessary and justified measure to:



- prevent a significant risk to the health and safety of the worker, or other workers;
- to determine a particular worker's fitness to work;
- to determine their entitlement to health-related benefits;
- to prevent discrimination on the grounds of disability or to assess the need to make reasonable adjustments; or
- to comply with other legal obligations.

We collect information through a medical examination or medical testing of workers if the testing is part of an occupational health and safety programme that workers have a free choice to participate in.

We make it clear early on in the recruitment process that we will only carry out medical examinations or testing once there is a likelihood that they will be appointed.

We limit the use of the information we collect for the purpose it was originally collected. We only carry out a different test on an existing sample, if the worker has been told about it and has freely consented.

We keep the information we have collected confidential, using an appropriate level of security.

We do not carry out the covert collection of bodily samples for testing.

We do not retain information obtained from medical examination or testing that is not relevant for the purpose(s) for which the examination or testing took place or for longer than is necessary.

### **Deciding when to collect information through drug and alcohol testing**

We are able to justify collecting information by testing workers for drug or alcohol use (eg for health and safety reasons).

We have made the rules and standards we may use tests to enforce clear to workers.

### **Carrying out drugs and alcohol testing**

We only use drug or alcohol tests where they provide significantly better evidence of impairment than other less intrusive means.

We use the least intrusive forms of testing that will bring the intended benefits to our organisation.

We tell workers what drugs they are being tested for.

- We base any testing on reliable scientific evidence about the effect of particular substances on workers.
- We limit testing to those substances and the extent of exposure that will meet the purpose for which the testing is conducted.
- We ensure random testing is genuinely random.
- We do not collect personal information by testing all workers, whether randomly or not, if only workers carrying out particular activity pose a risk.

[You can also view and print off this checklist and all the checklists of this guidance on our checklists page.](#)

# What if we use genetic testing?

## In detail

- [Can we use genetic testing on our workers?](#)
- [Can we ask a worker to disclose the results of a previous genetic test?](#)
- [Are there any circumstances we can use information from genetic testing?](#)
- [Checklist](#)

## 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.

Genetic testing has the potential to provide employers with information:

- predictive of the likely future general health of workers; or
- about workers' 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 needs to take a genetic test as a condition of employment.

You **should not** use genetic testing to collect information that is predictive of a worker's future general health. To collect 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.

### Further reading

For more information read our separate guidance on ['What is genetic data?'](#)

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

You **should 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. However, you **should** make the provision of the information voluntary.

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

You **should** avoid using genetic testing to obtain information unless, as a last resort, it is:

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

If you are using genetic testing to collect 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 you are using it.

It's important you 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 tested worker and make sure they can get professional advice.

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 worker. However, a DPIA is required where this processing is combined with certain other criteria.

### Further reading

For more detail see our [separate detailed guidance on data protection impact assessments](#) and in particular the section on '[What other factors might indicate likely high risk?](#)'.

## Checklist

- We avoid using genetic testing to collect information to make predictions of a worker's future general health. We only introduce genetic testing, if at all, after very careful consideration.
- We only use genetic testing as a last resort where it is:
  - clear that a worker with a detectable genetic condition is likely to pose a serious safety risk to others; or
  - known that a specific work environment or practice might pose a specific risk to workers with particular genetic variations; and
  - this is the only reasonable method to collect the required information.
- We carry out a data protection impact assessment if we want to process any genetic data.
- We only ask a worker to voluntarily provide information from their genetic test if it is relevant for our health and safety or other legal duties.

[You can also view and print off this checklist and all the checklists of this guidance on our checklists page.](#)

# What if we carry out health monitoring?

## In detail

- [What do you mean by health monitoring?](#)
- [When might we want to use health monitoring technologies?](#)
- [What do we need to consider if we want to monitor the health of workers?](#)
- [Can we ask workers to agree to the use of health monitoring technologies?](#)
- [Checklist](#)

## What do you mean by health monitoring?

This section considers some of the issues raised if you want to monitor the health of your workers. The focus here is on when your purpose is monitoring your workers' health on an ongoing basis.

You may have sector-specific or industry practices to follow, where you have specific duties and are required to monitor the health of your workers. For example, employers in the nuclear industry who need to monitor radiation exposure of their workers. You may also want to generally monitor your workers health using certain technologies.

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.

## When might we want to use 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. The information is then reported back to you or you have access to it. These technologies may also involve the use of automated decision making or artificial intelligence.

### Examples

The following are some examples of practices where employers may use technologies to monitor the health of their workers. These examples do not discuss any of the potential issues that may be involved in the deployment of such technologies, but are intended to illustrate some of the different ways an employer may use devices to monitor their workers' health.

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

A driver's company vehicle is fitted with a tachograph to record miles and time logged to ensure they

do not exceed safe limits on driving. The vehicle may also 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 offered a fitness app by their workplace as part of a scheme to promote healthier lifestyles and reduce sickness absence. The app allows workers to log their exercise and provides this personal information with the employer. The employer wants to collate and use the information to encourage participation in lunchtime fitness classes and other health activities, such as walking and cycling to work, eg through league tables and inter-team competitions. Workers may or may not receive some kind of reward or incentive if they use the app.

You may have an interest in ensuring the wellbeing of your workforce and may want to find ways to minimise staff absences resulting from ill-health. 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 **must** justify this as a proportionate and necessary measure to achieve your purpose. You **must not** use it in a way that is unfair or discriminatory to workers.

### Further reading

- [Video surveillance](#)
- [Automated decision-making and profiling](#)
- [Rights related to automated decision making including profiling](#)
- [Guidance on AI and data protection](#)
- [Explaining decisions made with AI](#)

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

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

You **must** identify a lawful basis and a special category condition for processing. Which lawful basis and special category condition are appropriate depends on your purpose(s) for the processing. For more information, read the sections '[What lawful bases might apply if we want to process workers' health information?](#)' and '[What special category conditions might apply?](#)'.

You **must** also consider your other data protection obligations. For more information, you should also read the section '[Data protection and workers' health information](#)' which details the data protection issues you

need to consider.

### Further reading

- [Data protection impact assessments](#)
- [Lawful basis for processing](#)
- [Special category data](#)

## 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. 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 you may consider using consent.

Remember, as health information is special category data, you **must** also meet a special category condition for processing. If you are offering genuine choice to your workers and seek to rely on consent as your lawful basis, then explicit consent may be appropriate as your condition for processing.

For a discussion on the use of consent, please see '[Can we rely on a worker's consent?](#)'.

### Example

An organisation wishes to offer their 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 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 can consider consent as their lawful basis. They can also consider explicit consent as their condition for processing, making sure to properly record and document the worker's consent.

### Further reading

For more information, see our [separate guidance on consent](#).

See also:

- [Lawful basis for processing](#)
- [Special category data](#)

## Checklist

- We only introduce health monitoring where it is a proportionate and necessary measure to address a particular issue, or where we have specific legal, industry or sectorial duties that require us to monitor the health of our workers.
- We ensure the health information collected from monitoring is not used in ways that is unfair or discriminatory to our workers.
- We carry out a data protection impact assessment if we want to introduce health monitoring of workers.
- We have identified a lawful basis for the monitoring and collection of workers' health information.
- We have identified a special category condition for the monitoring and collection of workers' health information.
- We have considered how the monitoring and use of the health information of our workers affects our other data protection obligations, such as accountability, data protection by design and default, and purpose limitation.
- We have considered how Article 22 applies if we are using automated decision making when monitoring the health of our workers.

[You can also view and print off this checklist and all the checklists of this guidance on our checklists page.](#)



# When can we share workers' health information?

## In detail

- [Can we share health information of our workers?](#)
- [How do we ensure the lawfulness of sharing?](#)
- [Can we share a worker's health information in an emergency?](#)
- [Can we disclose information about a worker's health to other workers?](#)
- [Checklist](#)

## Can we share health information of our workers?

Sometimes you may need to share health information about your workers. Data protection law does not prevent this, where it is appropriate to do so. This might be, for instance, as part of an occupational health referral, as part of 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 to help safeguard them.

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 sharing any 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 workers may expect confidentiality.

### Further reading

- [Data sharing page](#)
- [Data sharing code of practice](#)

## How do we ensure the lawfulness of sharing?

Before sharing any health information of a worker, you **must** identify at least one lawful basis. You **must** also identify a special category condition for processing. Which lawful basis and condition for processing are appropriate depends on your purpose for sharing the information. In order to comply with the accountability principle you **must** also show that you considered these before sharing the information.

For more information, please see ['What lawful bases might apply if we want to process workers' health information?'](#) and ['What special category conditions might apply?'](#).

For most information sharing, it is better not to rely on consent as the lawful basis, or explicit consent as the special category condition for processing. If you cannot offer a genuine choice, consent is not appropriate. Employers are often in a position of power over workers and therefore it's best to avoid relying on consent unless they are confident they can demonstrate it is freely given. Please see the section ['Can we rely on a worker's consent?'](#) for more information.

Depending why you need to share a worker's health information, other lawful bases such as legitimate interests or legal obligation are more likely to be appropriate. Similarly, the employment, social security and social protection law condition may be more appropriate as a special category condition for processing.

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

### Further reading

See our separate guidance on:

- [Lawful basis for processing](#)
- [Lawful basis interactive guidance tool](#)
- [Special category data](#)
- [Accountability principle](#)
- [Accountability Framework](#)

## Can we share a worker's 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 injures them and knocks 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 about this information to ensure that the worker receives appropriate care and treatment.

You **should** plan ahead as far as possible for dealing with urgent or emergency situations. Having an emergency plan in place that takes into account information 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 you may need to share your workers' health 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 **must** also consider how you will share the information securely. The best way to do this is through a data protection impact assessment (DPIA).

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

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 health information appropriately in an emergency situation.

### Further reading

See the [Data sharing code of practice](#) and in particular the section [Data sharing in an urgent situation or in an emergency](#).

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

You **should not** normally need to disclose a worker's health information with other workers, beyond those who genuinely need the information 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 a 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 in 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 freely consented to your disclosing 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 do so in such circumstances.

## Checklist

### Preparing to share workers' health information

- We have considered the purpose for sharing workers' health information and ensure that it is reasonable and proportionate to do so.
- We treat our workers fairly and do not use their health information in ways that would have unjustified adverse effects on them.
- We tell workers about why and how we propose to share their health information before or at the time we share it if this is not possible.

- We identify at least one lawful basis and a special category condition for processing before we share any health information.
- We avoid overly relying on consent to share workers' health information unless we can demonstrate it is genuine and freely given.

### **Sharing health information in an emergency**

- We have considered how we might need to share health information about workers in an emergency and considered developed a plan for doing so.
- We have considered what types of health information, how and when, and the risk involved in sharing and not sharing information as part of a data protection impact assessment.
- We have considered how we will share the health information securely.
- We have provided clear guidance and training to staff on when and how to share health information appropriately in an emergency.

### **Disclosing a worker's health information to other workers**

- We do not disclose a worker's health information to other workers unless they genuinely need the information to carry out their roles, or where there is a legal requirement to inform other workers for health and safety purposes.
- Where possible we avoid naming individual workers where there has been a communicable disease, but still let close contacts know they may have been exposed.

[You can also view and print off this checklist and all the checklists of this guidance on our checklists page.](#)

# Checklists

## At a glance

- These checklists provide an overview and quick guide to help you think about what you need to consider whenever you want to collect and use workers' health information. Read the guidance if you want a fuller explanation and understanding of the issues.
- These checklists are concerned with your data protection considerations only. They don't cover other separate legal obligations you may have as an employer, such as health and safety. You will need to obtain separate legal advice for any other such legal obligations.
- [Checklist: Data protection and workers' health information](#)
- [Checklist: Sickness and injury records](#)
- [Checklist: Occupational health schemes](#)
- [Checklist: Medical examinations and drugs and alcohol testing](#)
- [Checklist: Genetic testing](#)
- [Checklist: Health monitoring](#)
- [Checklist: Sharing workers' health information](#)

## Checklist: Data protection and workers' health information

- We have checked the processing of health information is necessary for the purpose we have identified and are satisfied there is no other reasonable and less intrusive way to achieve that purpose.
- We have identified a lawful basis for processing the health information.
- We have identified a special category condition for processing the health information.
- We avoid overly relying on consent when processing workers' health information unless we can demonstrate it is genuine and freely given
- We have documented what health information we are processing.
- Where required, we have an appropriate policy document in place.
- We have considered whether we need to do a data protection impact assessment.
- We ensure we only collect and use health information that is adequate, relevant and necessary and do not hold more than we need for the purpose.
- We included specific information about our processing of health information in our privacy information for workers.

- We have considered our retention policy on health information and keep the health information of workers only for as long as necessary.
- We ensure we keep the health information of our workers accurate, and where necessary, up to date.
- We put in place appropriate security measures to protection the health information of our workers.
- If we use health information of workers for automated decision making (including profiling), we have checked we comply with Article 22.
- We have considered how the use of the health information of our workers affects our other obligations such as accountability, data protection by design and default, and appointing Data Protection Officers (DPOs).
- We understand our obligations when workers exercise their data protection rights.

## Checklist: Sickness and injury records

- We distinguish between sickness, injury, and absence records.
- Where we only need to know information about the length of a worker's absence, and where practical, we consider using absence records instead of sickness records.
- We limit who can access and use information about workers from sickness and injury records, including whether they can have full access to the information of workers. We ensure they know what they can and cannot do with the health information.
- We only use sickness and injury records in ways that workers would reasonably expect.
- We have identified a lawful basis and a special category condition for processing sickness and injury records.
- We only share information from sickness or injury records about a worker's illness, medical condition or injury with third parties where it is necessary and proportionate to do so. For example:
  - there is a legal obligation;
  - it is necessary for legal proceedings; or
  - the worker has given explicit consent to the sharing.

## Checklist: Occupational health schemes

- We tell our workers how we intend to use information they provide as part of an occupational health scheme and the reports produced as a result. We also tell them who it might be made available to and why.
- We tell workers what data protection rights they have around the use of their information.
- We consider implementing a data sharing agreement with the occupational health provider, setting out under what terms information will be shared.
- We ensure that when requesting a worker's medical file as part of an occupational health referral, we handle any information received in accordance with data protection law.
- We don't ask workers to consent to the disclosure of their entire medical record, unless this is absolutely necessary.
- We avoid compromising any confidential communications between workers and health professionals in an occupational health service.

## Checklist: Medical examinations and drugs and alcohol testing

### **Deciding when to collect information through medical examinations and testing**

- We are able to justify collecting information through medical examination and testing of workers.
- We have made it clear to workers the rules and standards and when we may use tests to help enforce these.
- We carry out a data protection impact assessment to help document our purposes, justifications, safeguards, and how we intend to comply with our data protection obligations.
- We consider other less intrusive means of achieving our purposes, such as a health questionnaire instead of testing.

### **Carrying out medical examinations and testing**

- We tell workers what they are being tested for, the frequency of testing, and the consequences of the results.
- We use the least intrusive forms of medical examination and testing that will bring the intended benefits to our organisation.

- We ensure that the testing method is of good quality, reliable and provides accurate results.
- We only collect information if it is a necessary and justified measure to:
  - prevent a significant risk to the health and safety of the worker, or other workers;
  - to determine a particular worker's fitness to work;
  - to determine their entitlement to health-related benefits;
  - to prevent discrimination on the grounds of disability or to assess the need to make reasonable adjustments; or
  - to comply with other legal obligations.
- We collect information through a medical examination or medical testing of workers if the testing is part of an occupational health and safety programme that workers have a free choice to participate in.
- We make it clear early on in the recruitment process that we will only carry out medical examinations or testing once there is a likelihood that they will be appointed.
- We limit the use of the information we collect for the purpose it was originally collected. We only carry out a different test on an existing sample, if the worker has been told about it and has freely consented.
- We keep the information we have collected confidential, using an appropriate level of security.
- We do not carry out the covert collection of bodily samples for testing.
- We do not retain information obtained from medical examination or testing that is not relevant for the purpose(s) for which the examination or testing took place or for longer than is necessary.

### **Deciding when to collect information through drug and alcohol testing**

- We are able to justify collecting information by testing workers for drug or alcohol use (eg for health and safety reasons).
- We have made the rules and standards we may use tests to enforce clear to workers.

### **Carrying out drugs and alcohol testing**

- We only use drug or alcohol tests where they provide significantly better evidence of impairment than other less intrusive means.
- We use the least intrusive forms of testing that will bring the intended benefits to our



organisation.

- We tell workers what drugs they are being tested for.
- We base any testing on reliable scientific evidence about the effect of particular substances on workers.
- We limit testing to those substances and the extent of exposure that will meet the purpose for which the testing is conducted.
- We ensure random testing is genuinely random.
- We do not collect personal information by testing all workers, whether randomly or not, if only workers carrying out particular activity pose a risk.

## Checklist: Genetic testing

- We avoid using genetic testing to collect information to make predictions of a worker's future general health. We only introduce genetic testing, if at all, after very careful consideration.
- We only use genetic testing as a last resort where it is:
  - clear that a worker with a detectable genetic condition is likely to pose a serious safety risk to others; or
  - known that a specific work environment or practice might pose a specific risk to workers with particular genetic variations; and
  - this is the only reasonable method to collect the required information.
- We carry out a data protection impact assessment if we want to process any genetic data.
- We only ask a worker to voluntarily provide information from their genetic test if it is relevant for our health and safety or other legal duties.

## Checklist: Health monitoring

- We only introduce health monitoring where it is a proportionate and necessary measure to address a particular issue, or where we have specific legal, industry or sectorial duties that require us to monitor the health of our workers.
- We ensure the health information collected from monitoring is not used in ways that is unfair or discriminatory to our workers.
- We carry out a data protection impact assessment if we want to introduce health monitoring of

workers.

- We have identified a lawful basis for the monitoring and collection of workers' health information.
- We have identified a special category condition for the monitoring and collection of workers' health information.
- We have considered how the monitoring and use of the health information of our workers affects our other data protection obligations, such as accountability, data protection by design and default, and purpose limitation.
- We have considered how Article 22 applies if we are using automated decision making when monitoring the health of our workers.

## Checklist: Sharing workers' health information

### **Preparing to share workers' health information**

- We have considered the purpose for sharing workers' health information and ensure that it is reasonable and proportionate to do so.
- We treat our workers fairly and do not use their health information in ways that would have unjustified adverse effects on them.
- We tell workers about why and how we propose to share their health information before or at the time we share it if this is not possible.
- We identify at least one lawful basis and a special category condition for processing before we share any health information.
- We avoid overly relying on consent to share workers' health information unless we can demonstrate it is genuine and freely given.

### **Sharing health information in an emergency**

- We have considered how we might need to share health information about workers in an emergency and considered developed a plan for doing so.
- We have considered what types of health information, how and when, and the risk involved in sharing and not sharing information as part of a data protection impact assessment.
- We have considered how we will share the health information securely.

We have provided clear guidance and training to staff on when and how to share health information appropriately in an emergency.

### **Disclosing a worker's health information to other workers**

We do not disclose a worker's health information to other workers unless they genuinely need the information to carry out their roles, or where there is a legal requirement to inform other workers for health and safety purposes.

Where possible we avoid naming individual workers where there has been a communicable disease, but still let close contacts know they may have been exposed.