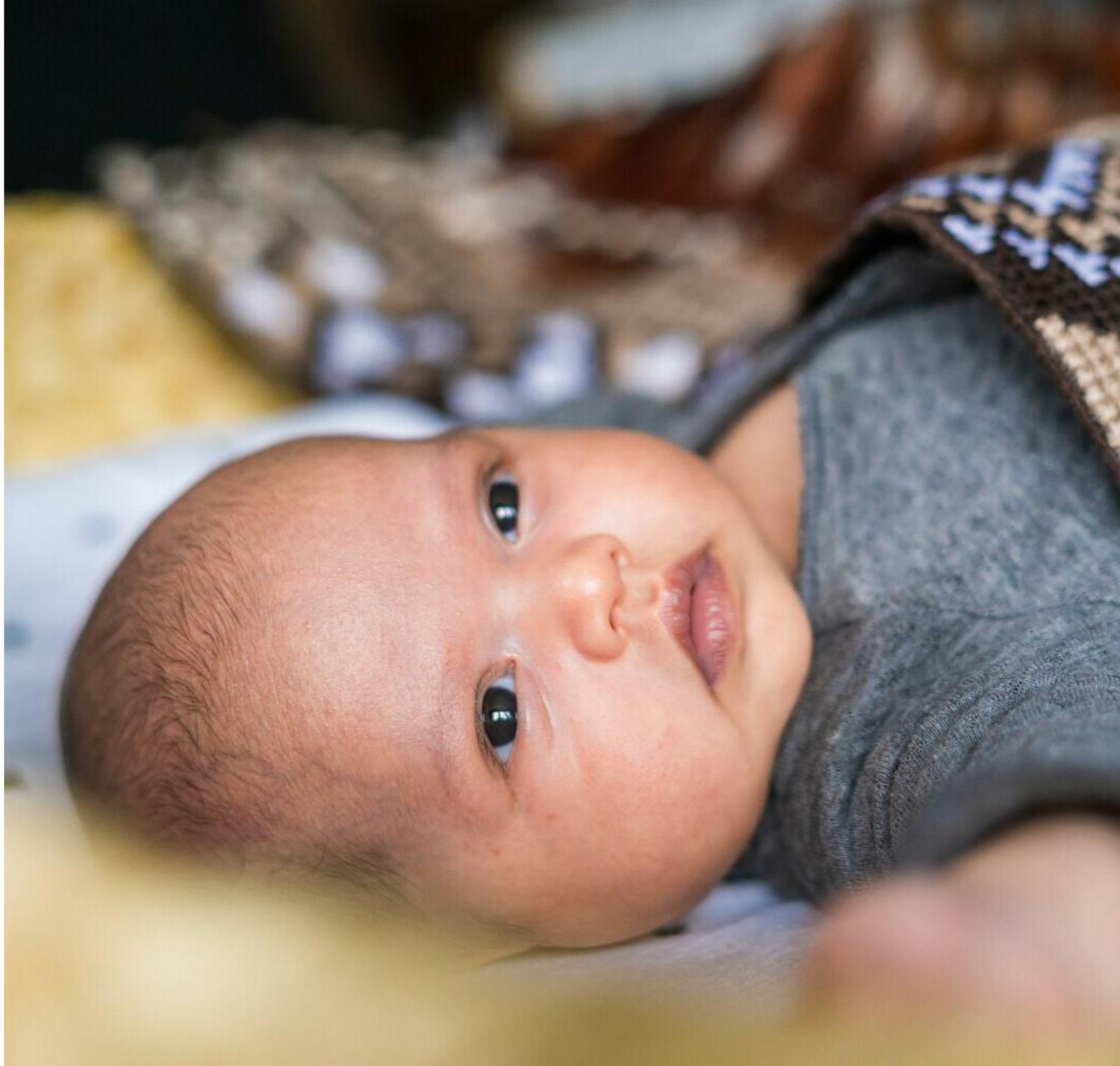
Privacy Commissioner
Te Mana Mātāpono Matatapu

Health ABC

An introduction to protecting health information under the Health Information Privacy Code.

2025



This module is also online

The content used here comes from the Health ABC e-learning module at privacy.org.nz. It is free to use.

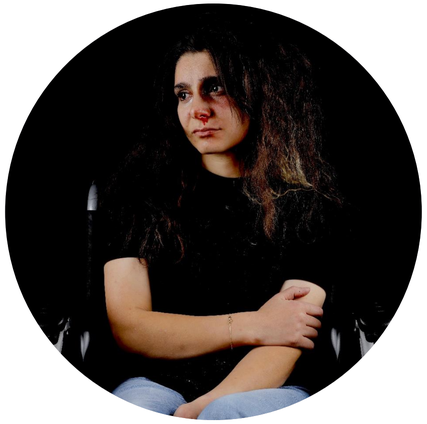
What to collect when you’re collecting

This section gives you an understanding of what health information you can collect from people.

What to collect when you’re collecting

As a health or disability professional, you need information about your patients or clients to do your job. The Health Information Privacy Code (the Code) sets rules on what you can ask for, how you can get it, and how you can use it.

The Code allows you to collect information if you need it for a purpose connected to what your agency goes. The rule of thumb for collecting information is: only collect information you need to do your job.



EXAMPLE

A patient visits a GP for the first time. They have a bruise on their arm that is taking a long time to heal. The GP looks at the bruise. They also measure the patient's height, weight, and blood pressure.

The GP is responsible for a wide range of health services, so it is appropriate for her to collect information related to aspects of health other than just the bruise.

What you can’t collect

Bear in mind that you can only collect information related to your job. The nature of healthcare is that this definition may be very wide. You **cannot collection information that** is not related to the service you provide.

LEARNING CHECK

A person goes to a counsellor to talk through their recent separation from their partner. The counsellor asks if they've gained or lost weight since the separation. Is this appropriate?

Yes - that's appropriate. Shifts in weight can be an indicator of general wellbeing, so it’s relevant to the services the counsellor provides.

LEARNING CHECK

A person goes to a counsellor to talk through their recent separation from their partner. The counsellor asks how much the person weighs. Is this appropriate?

No - this is less likely to be appropriate, although it may be appropriate in some circumstances. For example, if they had an eating disorder as well, it would be appropriate for the counsellor to ask about their weight.

Learning check

A person is at a clinic to discuss ways they can lose weight. The nurse who assesses them asks what kind of food they eat each day.

Is that appropriate?

Yes - since the clinic is working on weight loss, its staff need to know what kind of food people are eating in order to recommend changes.

Privacy statements and using information

In this section you'll look at the connection between privacy statements and how you use the health information you collect.

Privacy statement

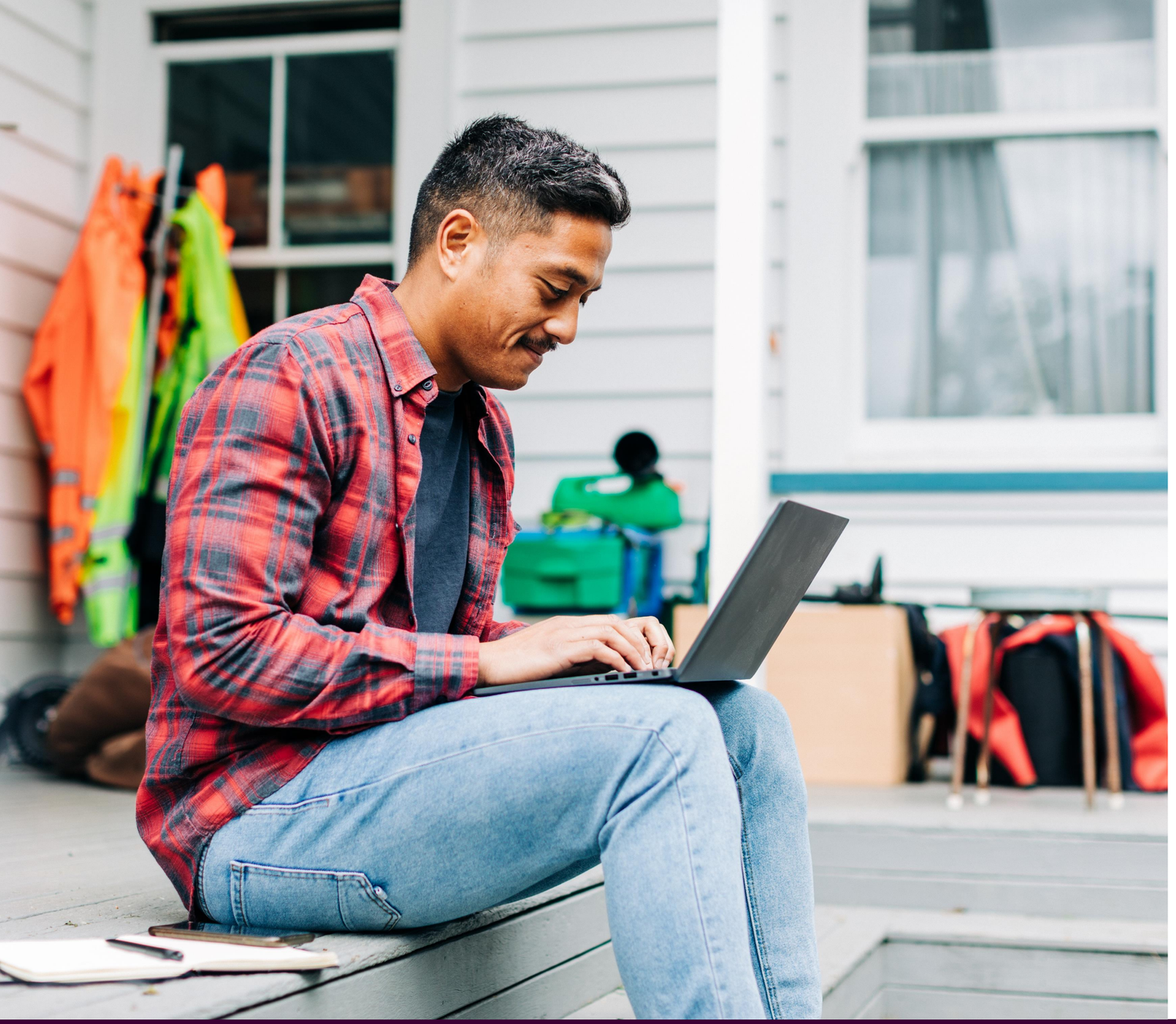
When you ask people for their information, you need to tell them what you're asking for, why you're asking for it, and what you'll do with it. This is often done through a privacy statement.

Then, when you use their information, you can use it for the reasons you have given when you collected it.

STATEMENT TIP

Make your privacy statements broad, to make your job easier later.

The more your statement covers, the less time you have to spend asking for permission later. But make sure you follow what you learned in the first section about only collecting the information you need.



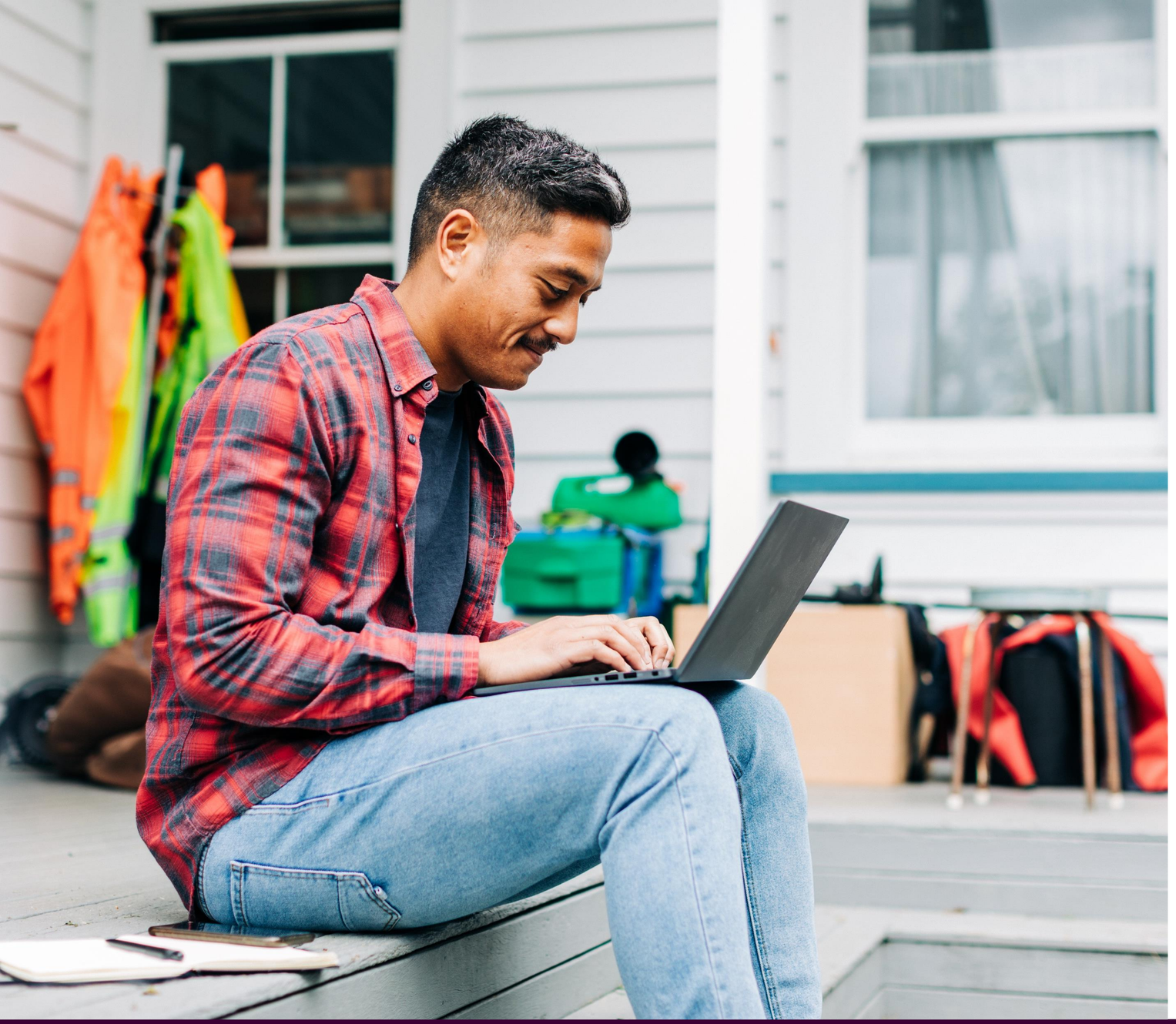
Learning check

A physiotherapy clinic routinely refers patients to a radiology lab for X-rays and other imaging services. To do so, it needs to send patient records to the lab.

Which of these statements would be the most useful for the clinic?

A. "We will use your personal information to provide physiotherapy services, and we will not share it without your permission."

B. "We will use your personal information to provide physiotherapy services. This many involve sharing your information with other organisations, such as radiology labs."



Learning check

B is the correct answer because it lets the clinic share information with other organisations in order to provide physiotherapy services.

This means that if they want to refer someone to a radiology lab, they don't have to seek the person's permission.

Referring patients to labs is an aspect of physiotherapy services, so using the information this way is consistent with the purpose that was explained to the patient in the privacy statement.

Being fair and reasonable

In this section you'll learn about what you need to consider in order to collect health information in a way that is not unfair or overly intrusive.

Unfair or intrusive

Rule 4 of the Health Information Privacy Code (the Code) says that you cannot collect information in ways that are unfair, or intrude too much on someone's affairs.

You need to take particular care to be fair and reasonable when collecting information from children and young people.

EXAMPLE

J works as a nurse at a surgical specialist's office. A new patient has filled out some forms, and is sitting in the busy waiting area.

J notices that the patient has forgotten to answer some of the questions on the form. Since the patient is in the waiting room, J goes out and asks the questions in person. The patient then has to answer their questions in a waiting room full of people. This could be a privacy breach - and it's also not very nice.

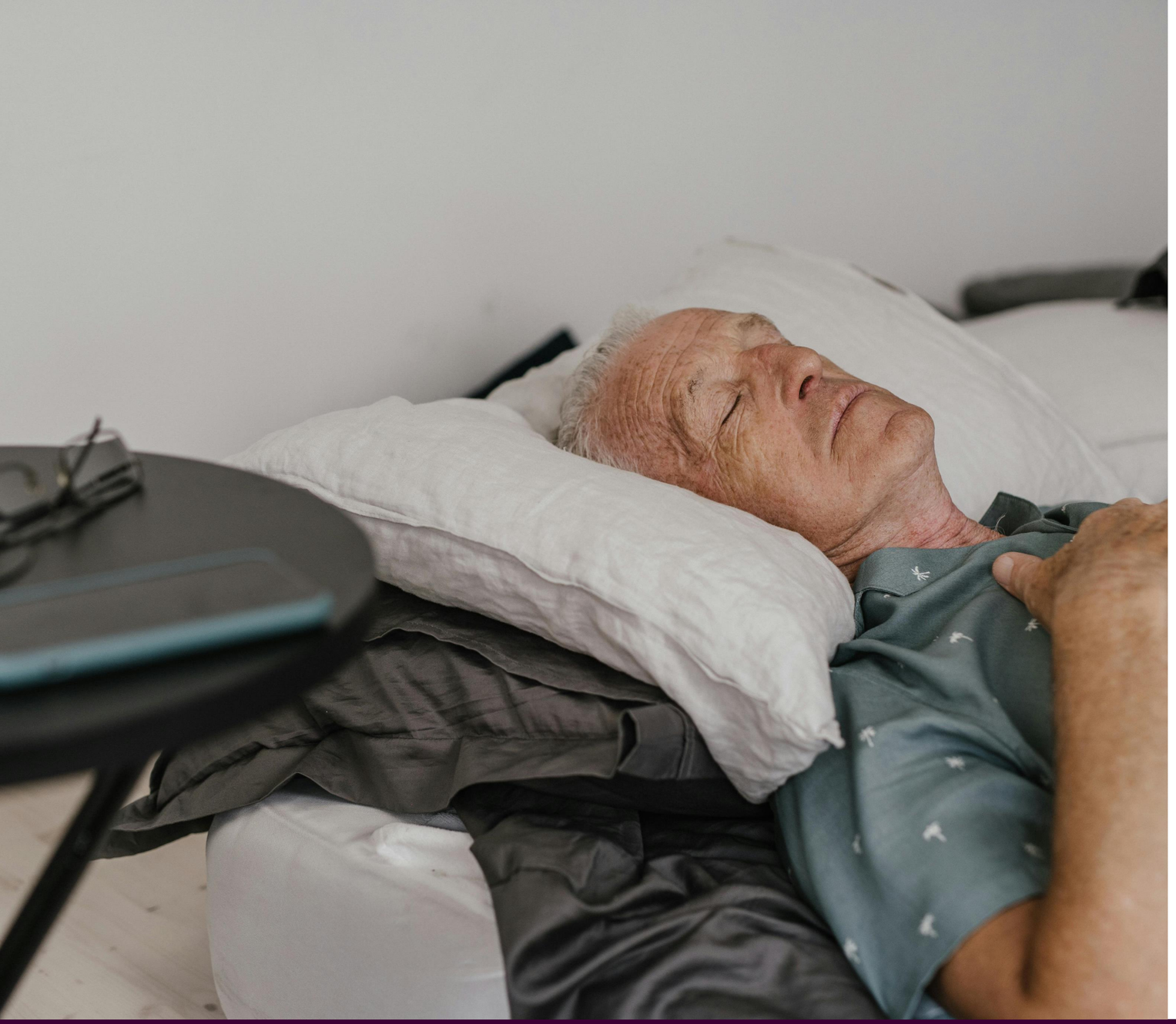
J can ask for the information, because they need it to provide health services to the patient. But J also needs to think about how they're asking for the information to make sure they're being fair and reasonable.

Discreet options

J could get the information in a different way. For example.

1. They could ask the patient to join them in a private room, then ask for the missing information. This would protect the person from having their personal information overheard.
2. J could put the form in front of the patient, give them a pen, and ask them to fill out the remaining fields, without saying what information is in the fields. This way, the patient can provide the information without saying it out loud.
3. J can send the blank form through to the doctor, and let the doctor ask the remaining questions. This is similar to the first approach, in that the patient can safely provide the information without risk of being overheard.

All three of these would be more fair and reasonable than asking for the information in the public waiting room, so it is up to J to choose an approach that works for them.



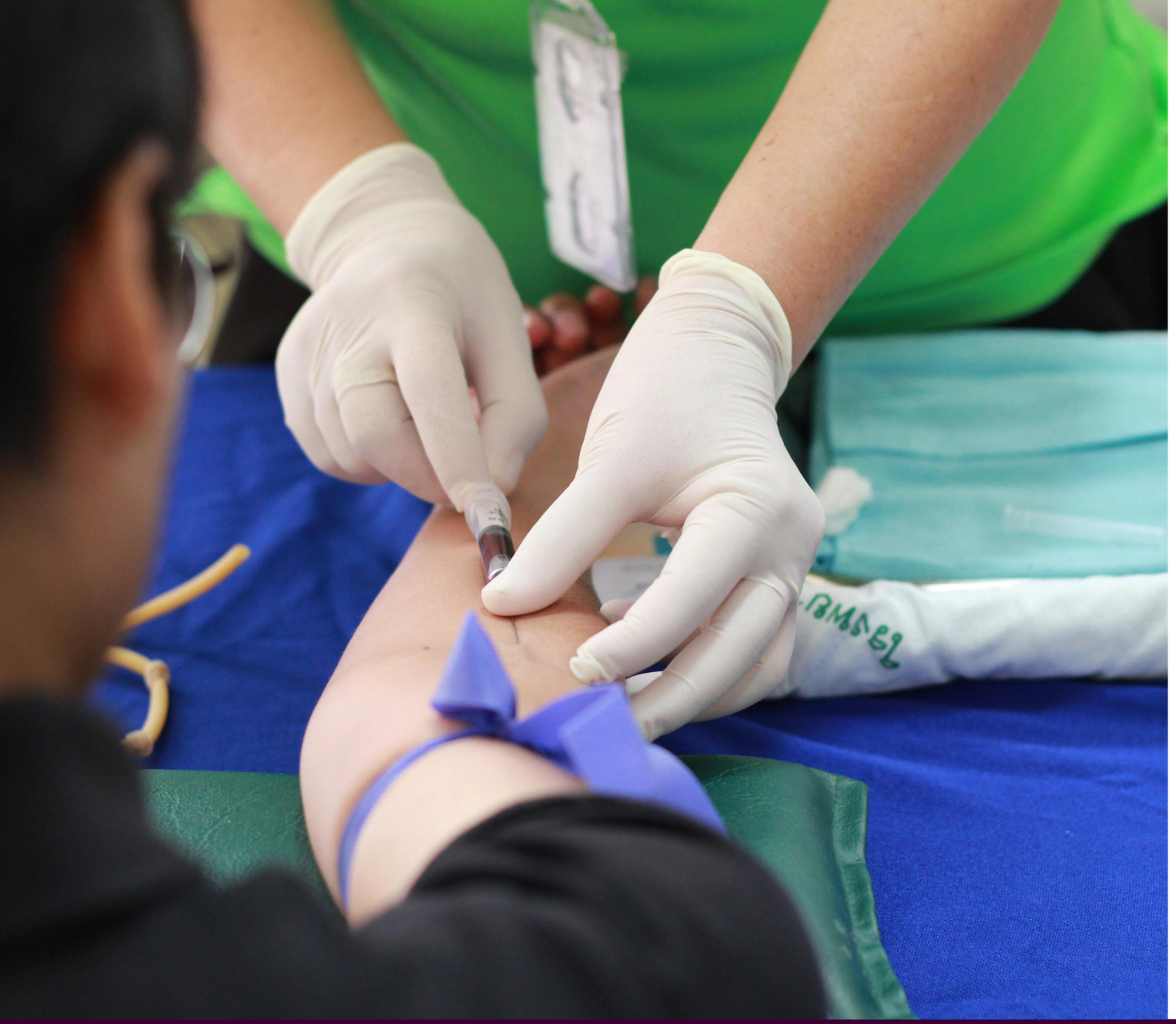
Meet S

Health professionals also need to make sure they don't collect information in a way that intrudes too much on someone's personal affairs.

S works at a rest home as a caregiver. They need a urine sample from a resident. They hand the resident a cup to urinate in, and ask if they can go to the bathroom to fill it. The resident doesn't move every fast, and S is in a rush so tells S they will need to fill the cup from their bed, in front of them.

This could definitely be a privacy breach. Even though there's nothing wrong with asking for a urine sample in some circumstances, the way you collect it can make a difference.

In this case, the way the nurse collected the sample would be likely to be unreasonably intrusive.



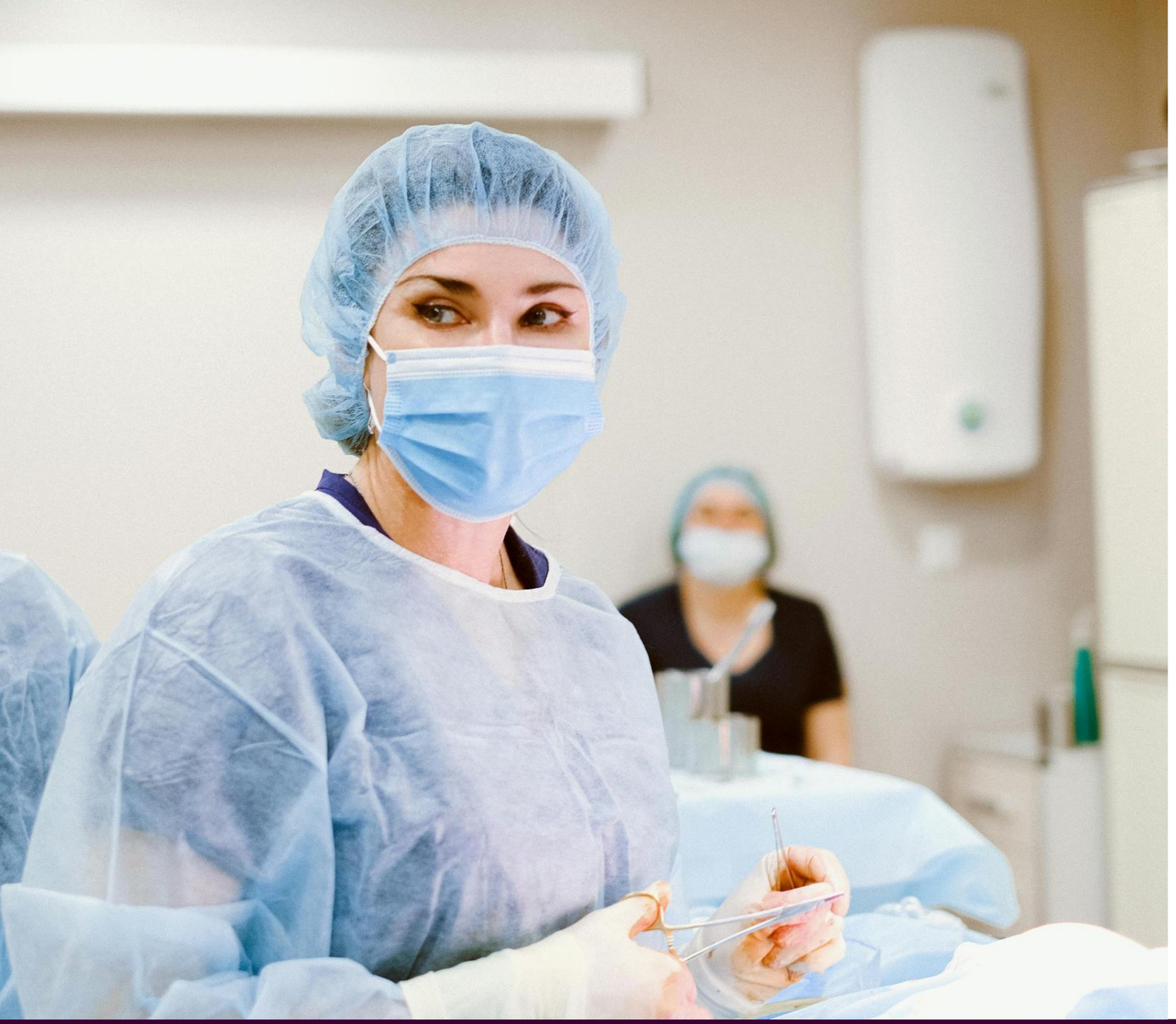
Learning check

A health insurance company has contracted a nurse to make house calls.

The nurse needs to take a blood test. They are only available during working hours, so they tell their patient that they'll need to meet them at their office and that they should book a meeting room.

Is this appropriate?

No. This could be unfair, because it intrudes on the patient’s employment. The nurse can give the patient the option of having the blood test at work, but it would be inappropriate to require that the nurse be invited to the patient's office.



Learning check

An anaesthetist is pre-assessing an adult patient for their surgery. They need to ask the patient a series of lifestyle questions. The patient has brought a friend (also an adult) with them, and the anaesthetist goes ahead and asks the questions while the friend is in the room.

Is this appropriate?

No. Questioning in front of a friend would be unfair. The anaesthetist should give the patient the option to have their friend wait outside before they ask personal questions.

Learning check

A new patient comes into a GP's office with a sore ear, and the GP asks how many sexual partners the patient has had over the past month.

Is that appropriate?

No. This seems unnecessarily intrusive in these circumstances, because the patient has come in with a specific problem. Sexual history is inherently sensitive information, so a GP needs a good reason to ask about it.

A patient comes into a GP's office with a sore ear and the GP takes their temperature.

Is this appropriate?

This would be appropriate, because a patient's temperature would be useful for diagnosing a sore ear. Taking a temperature in a doctor's office would also be a fair way to collect this information.

Keeping information safe

In this section you'll learn about your obligations and responsibilities when storing health information.

Keep information safe

When you hold someone's personal information, you need to take reasonable steps to keep that information safe.

The key to this requirement is 'reasonable' steps. The Health Information Privacy Code only requires you to take reasonable steps to keep information safe. It does not require you to keep information safe at all costs.

The general rule of thumb about what 'reasonable' is, is that more sensitive information requires more steps to keep it safe. Health information will often be sensitive, so you will likely need to take more steps to keep it safe than you might with other types of information.

MEET J

J has an administrative job in the cancer ward at a hospital. J's teenager has just started dating T who their parent suspects is a drug user.

J logs into the system and quickly looks up T's medical records. They find that T has been admitted for problems related to drug use in the past. J calls their teenager and tells them what they've found out.

J's colleague overhears the phone call and makes a complaint to their supervisor. Their supervisor starts a disciplinary process, and J's employment is terminated.

Keep information safe

When you hold someone's personal information, you need to take reasonable steps to keep that information safe.

The key to this requirement is 'reasonable' steps. The Health Information Privacy Code only requires you to take reasonable steps to keep information safe. It does not require you to keep information safe at all costs.

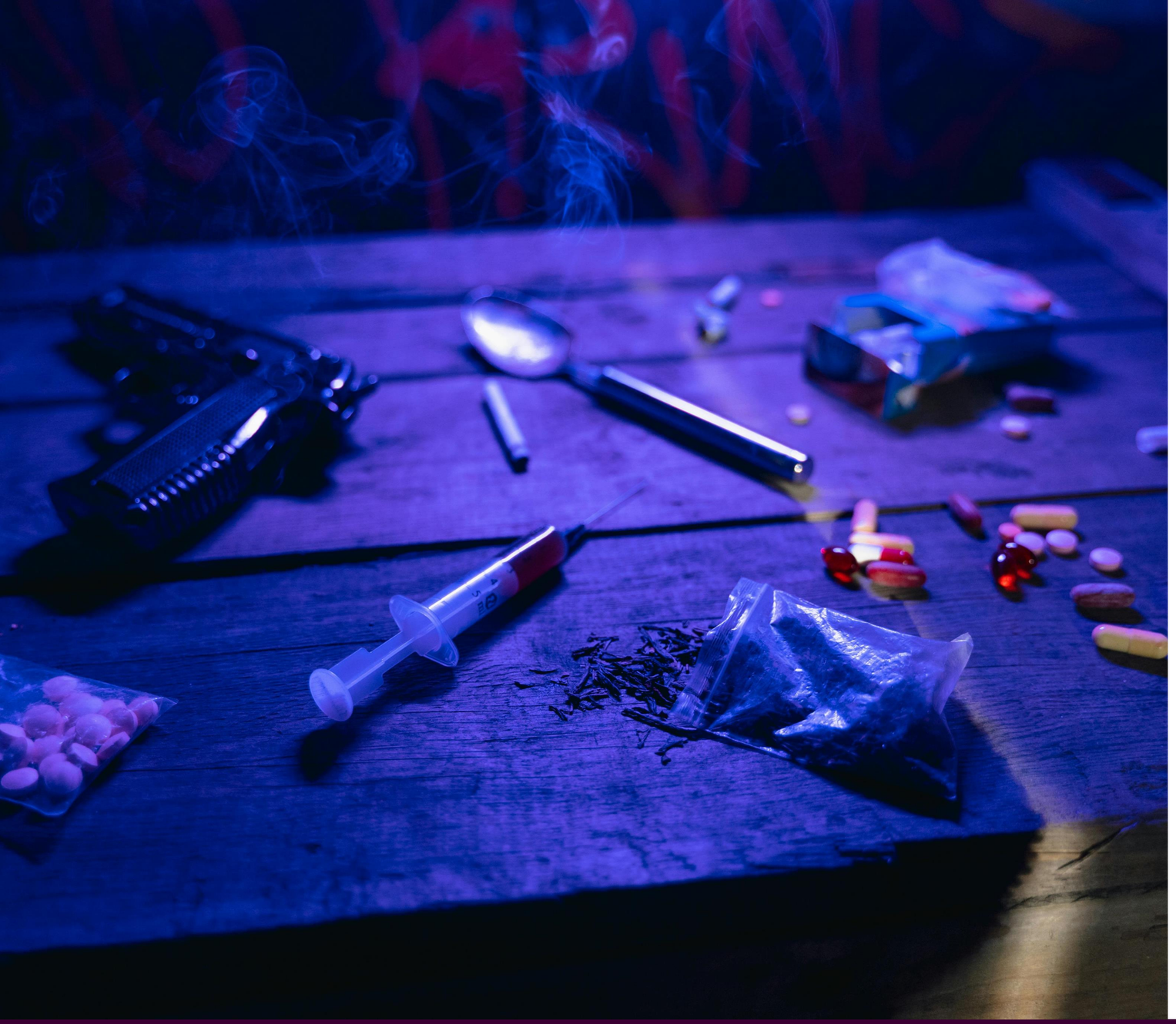
The general rule of thumb about what 'reasonable' is, is that more sensitive information requires more steps to keep it safe. Health information will often be sensitive, so you will likely need to take more steps to keep it safe than you might with other types of information.

MEET J

J has an administrative job in the cancer ward at a hospital. J's teenager has just started dating T who their parent suspects is a drug user.

J logs into the system and quickly looks up T's medical records. They find that T has been admitted for problems related to drug use in the past. J calls their teenager and tells them what they've found out.

J's colleague overhears the phone call and makes a complaint to their supervisor. Their supervisor starts a disciplinary process, and J's employment is terminated.



Who is responsible?

In this scenario, if J's teenager's partner made a privacy complaint, the hospital could still be found to have breached their privacy, even though it acted the minute it found out what J had done.

This is because the only reason it found out was because J's colleague overheard them on the phone.

There were no systems in place to stop or manage this kind of behaviour in the first place.

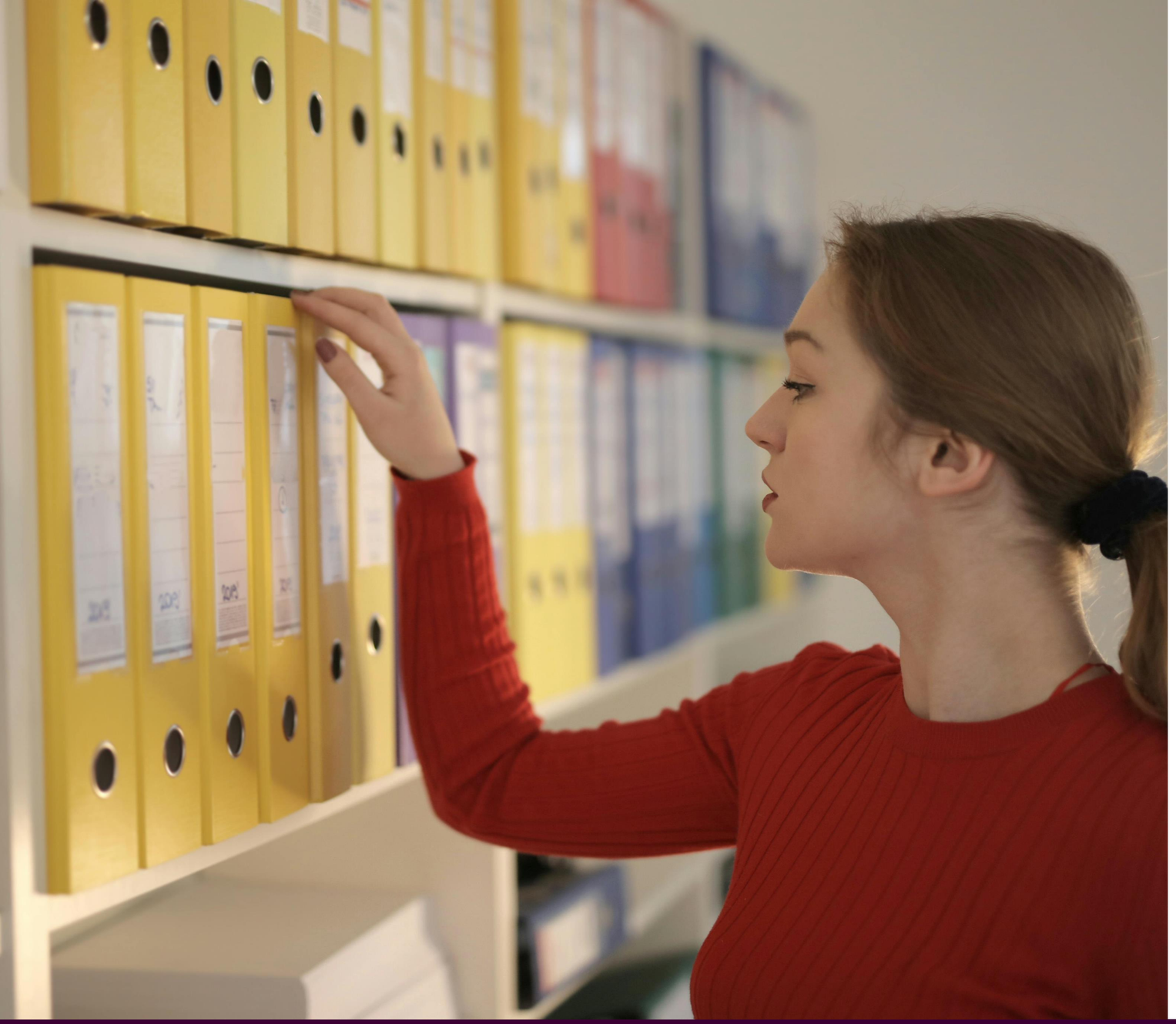
Reasonable steps

1. Restrict access so that staff can only look up information they need for their specific job. Since the teenager's partner has never had cancer, J probably wouldn't need access to their records.
2. Carry out random audits of employee browsing behaviour.
3. Allow staff to look up any record, but build a system that 'flags' when they look up records of people outside their area.
4. Hold training sessions about privacy obligations on a regular basis.
5. Routinely remind staff members about their privacy obligations.

Relying on colleagues overhearing conversations and telling their supervisors is not likely to be enough.

When people want to see their own information

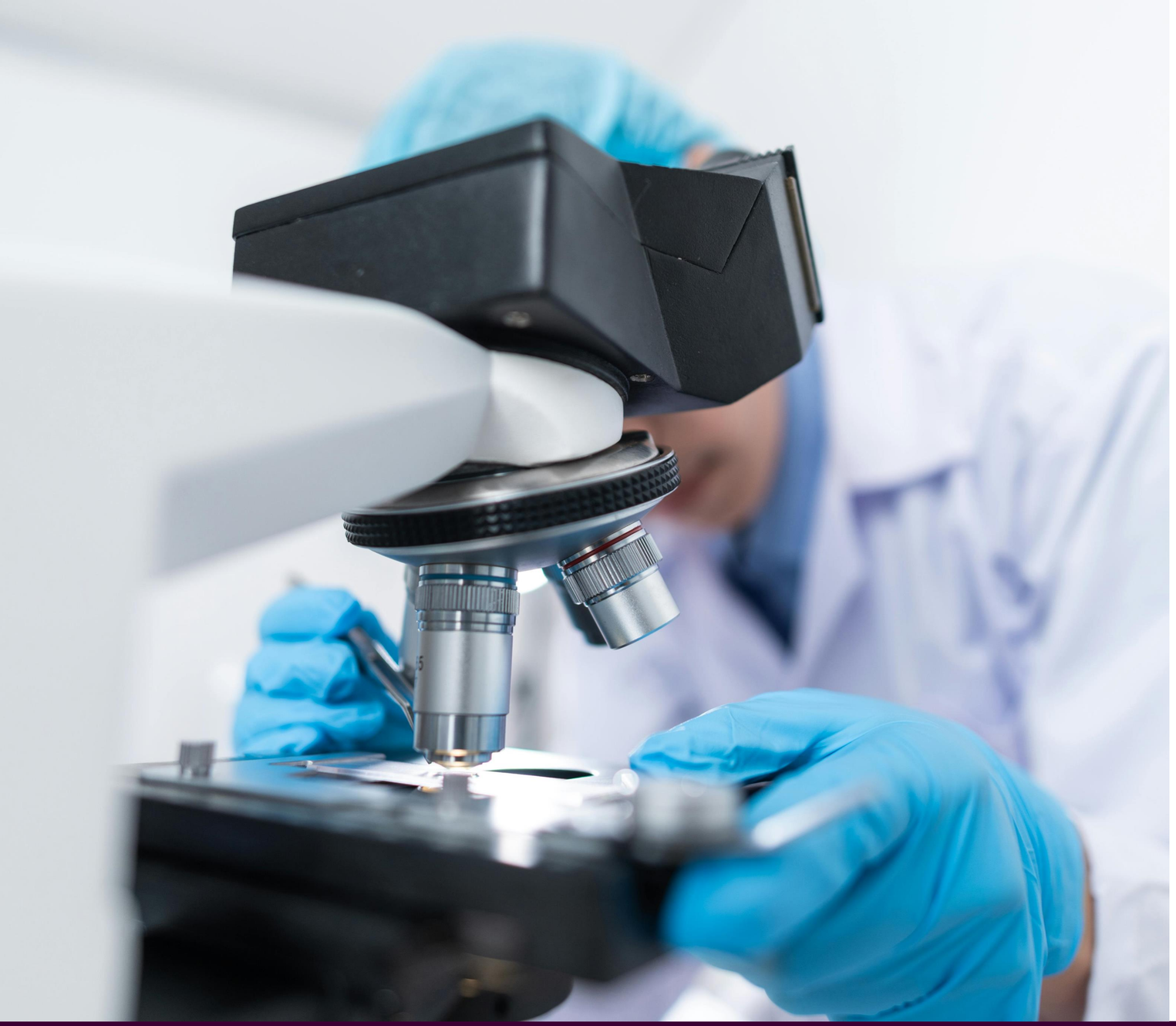
In this section you'll learn about your obligations when people ask to see the information you hold about them.



Information requests

The Health Information Privacy Code gives people the right to see their own information. In most cases, you must do the following:

1. Confirm whether you have the information
2. Give it to the person as soon as possible
3. Give it to the person for free.



Test results

Test results are a common example of health information that people want to see.

Two years ago, M had some blood tests. Now, they want to see the results, so they call their GP office and ask for them.

This information is in M's file and the GP's office is able to quickly find the information M wants, then email it to them.

Learning check

J has started a new job, and needs proof of their vaccinations. They call their GP's office on a Monday and ask for the records.

The GP has them, but the records are old and they're in the paper file. The office won't have time to look for them and photocopy them until Friday.

How should the office respond?

A. Tell J that they have the records but it's too hard to get them.

B. Tell J that they have the records, and that J will get the records in a few days.

The correct answer is B. The records are available, and a few day's delay is as fast as is practical in this situation.

Some is better than none

Sometimes it's not easy to satisfy someone's information request. There are a number of cases where it may be difficult, or impossible, to give someone their personal information.

Some of the more common examples are:

- The information is too hard to find.
- The information doesn't exist.
- Giving the person the information would breach someone else's privacy.

In theses cases, you should try to find a way to give the patient some of their health information.

There are more exceptions to this rule. Our Ask Us database has a question called, 'When can I refuse access to personal information?', which has more detail. As does our longer health e-learning module Health 101, which can be completed online at https://elearning.privacy.org.nz

Learning check

D goes to group therapy, where the counsellor takes extensive notes. After a few weeks, D asks to see these notes, as they contain information about them.

These notes contain information about D, but they also contain information about the other people in the group therapy session.

What should the counsellor do?

A. Give the notes to D as they are.

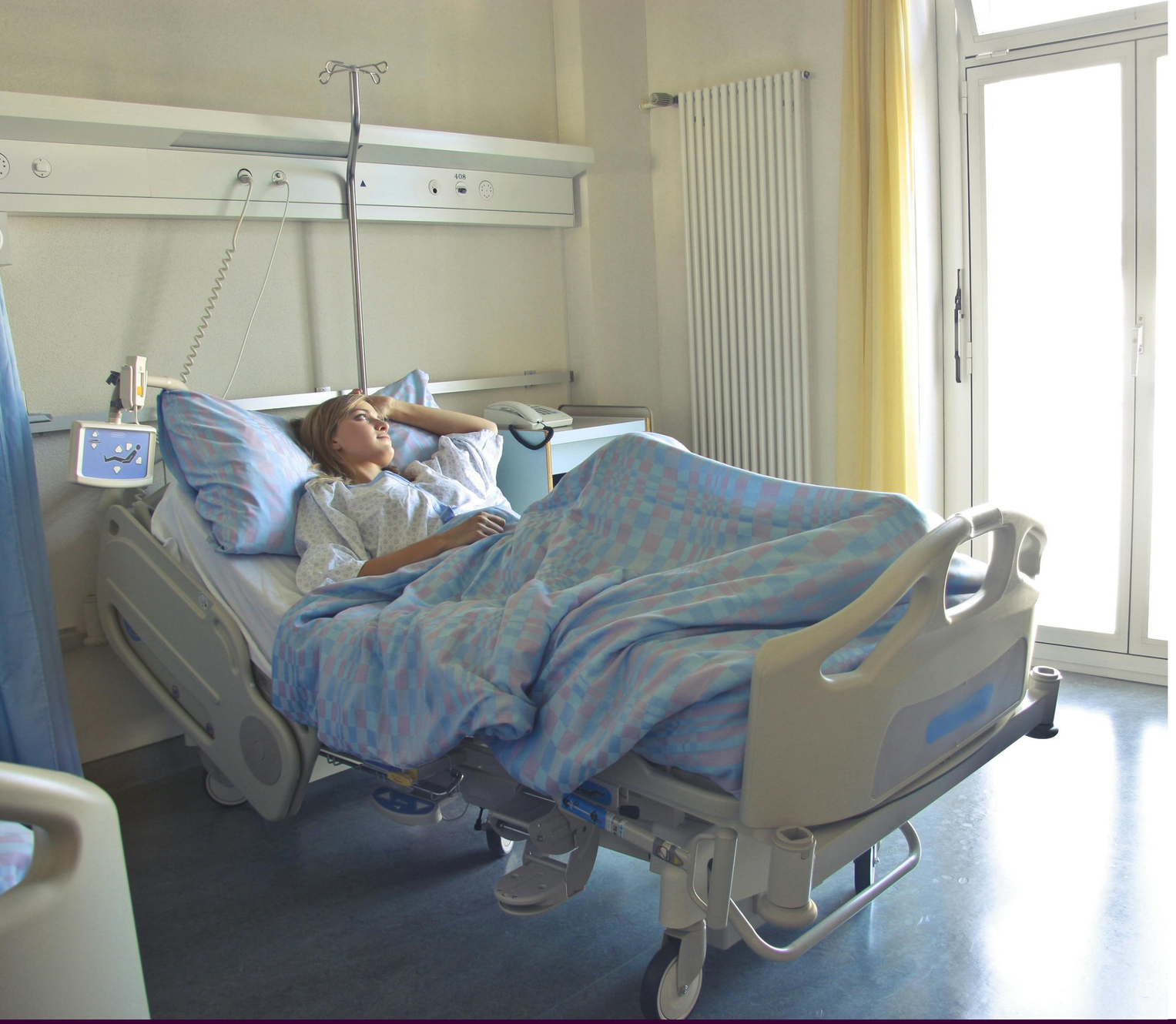
B. Give the notes to D, but take out anyone else's personal information.

C. Refuse to give anything to D.

B is the correct answer. Taking out other people's information lets the counsellor give D their information without intruding on someone else's privacy. The counsellor could do this by making a photocopy of the notes, then carefully removing or deleting other people's personal information.

When people want to change their information

This section explains your obligations when people ask to correct their information that they think is wrong.



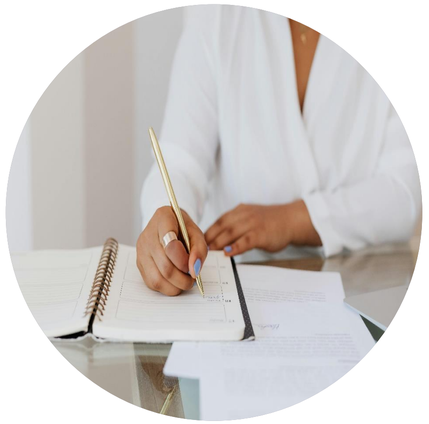
Learning check

R becomes very unwell after they eat some bad meat. The hospital diagnoses them with botulism. Six weeks later, a sample of the meat comes back from the pathology lab, where it has tested negative for botulism.

R asks the hospital to change their records, and remove the diagnosis of botulism. Does the hospital have to change the records?

No, they don't. The medical records show what the diagnosis was at that time, based on the information they had at that time. If R wants, they can attach a note to the initial diagnosis clarifying that they ultimately did not have botulism.

Condition change



G previously had a long-term medical condition that they feel they've recovered from.

They notice that the condition is still listed as a current condition in their GP's patient portal. They ask the GP to remove the health condition completely from their file because they believe it's not right. The GP considers that the past medical condition is still clinically relevant to the person's future healthcare.

What should the GP's office do?

A. Tell the person that the GP won't remove the medical condition because they believe it's still relevant to their healthcare.
B. Move the medical condition to the "past conditions" part of the patient portal and add a note that the patient believes the information is no longer correct.

B is the correct answer. Even though the GP considers that the medical condition is still clinically relevant, the person has a right to a note explaining their health information.

When you think there’s a threat

In this section you'll learn about what you can do when you think someone is a threat to themselves or to somebody else.

Serious threat

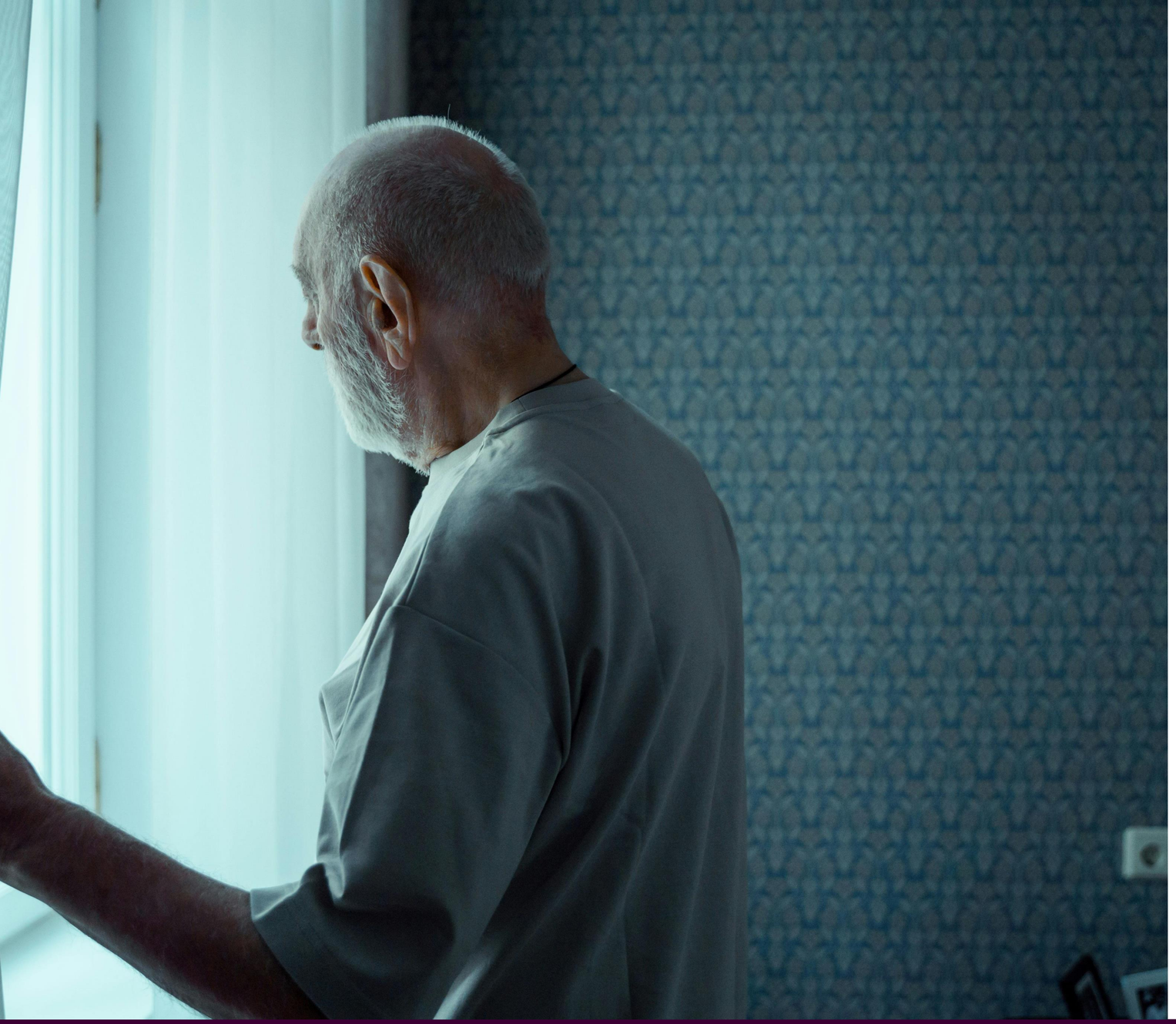
You can share information about people when you think there is a serious threat. A serious threat is when someone's life or health is in danger.

In these situations, you need good reasons to think that there is a threat, but you are allowed to be wrong.

WHAT IS A SERIOUS THREAT?

To assess whether there is a good reason to disclose someone's information, you should think about:

1. How likely the threat is.
2. How severe the consequences would be if the threat was carried out.
3. When the threat may happen.



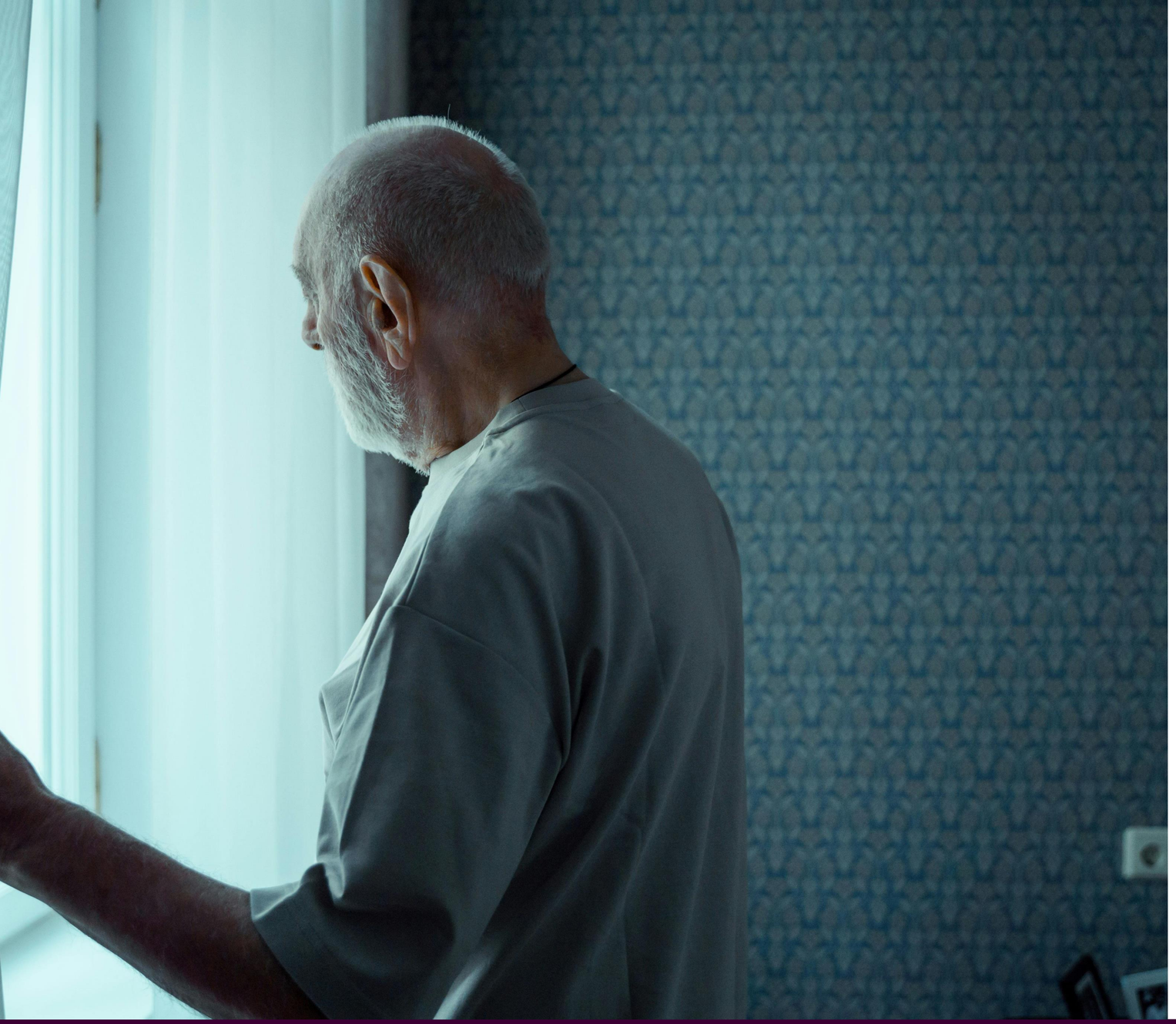
Meet R

R is a care worker for the elderly who has several clients in the community. They go into people's homes a couple of times a week to help with day-to-day tasks, such as the shopping, cleaning, and preparing meals.

One of R's clients is an older person named L.

One day, L tells R that he's feeling very lonely, and is thinking about killing himself. L also outlines how they would do it. He swears R to secrecy.

What are R's options for what can be done next?



R’s options

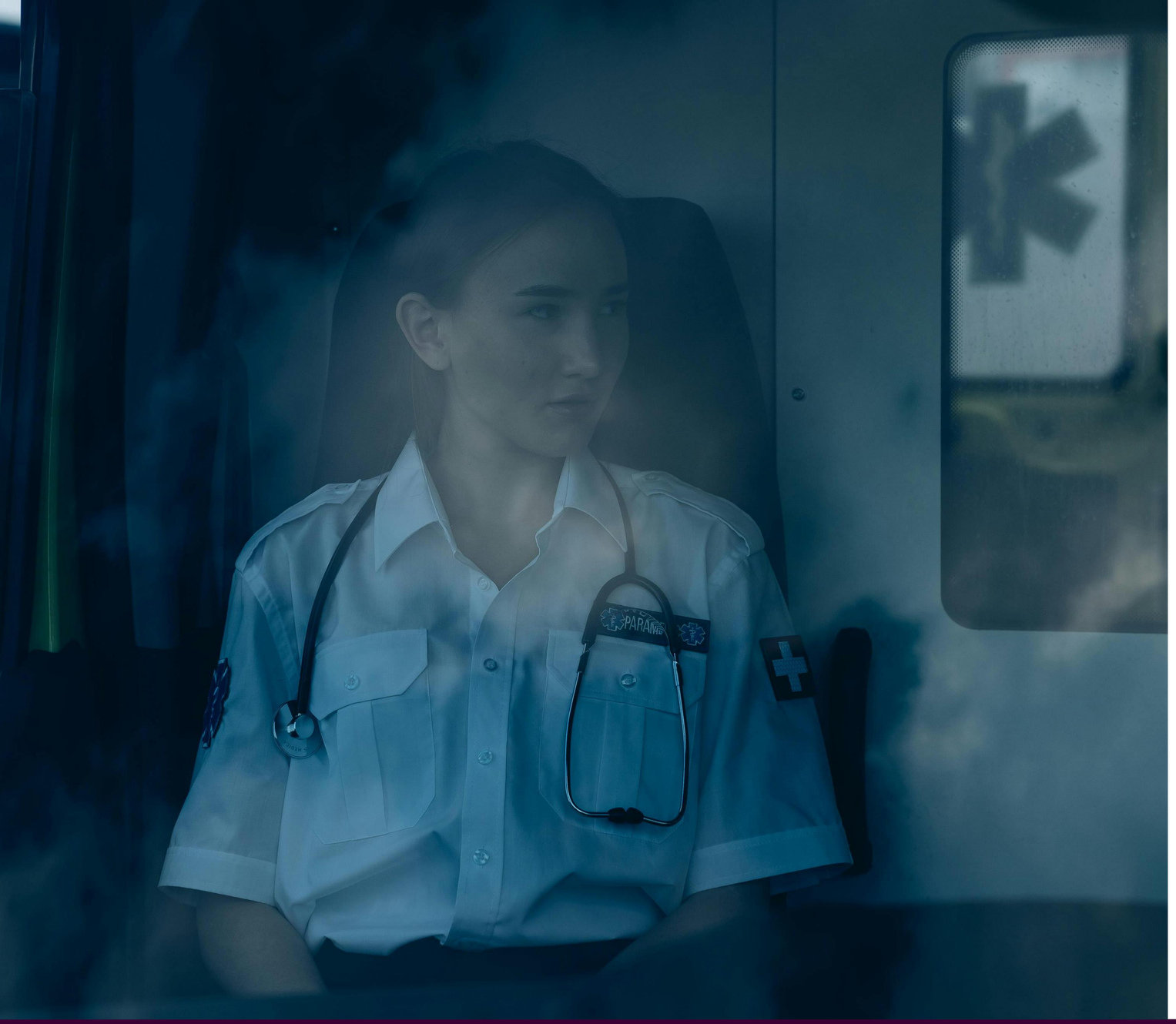
This is clearly a serious threat:

LIKELIHOOD: R does not know exactly how likely the threat is, but it is more likely than if L had told him nothing.

CONSEQUENCES: The consequences are very severe - L's life is potentially at stake.

WHEN MIGHT THIS HAPPEN: R does not know when this might happen.

Since the consequences are potentially so severe, R decides to tell someone, even though they don't know exactly how likely it is, or when it might happen. This is allowed under the Code.



Who to tell?

R now needs to decide who to tell about this threat. The rule of thumb is that you should only tell someone who can do something to prevent the threat.

Some options could include:

- The Police
- A social worker who works with R
- R's own supervisor
- The local mental health crisis team (if R doesn't know how to contact his local crisis team, he can ring Healthline on 0800 611 116).

The person he tells doesn't need to be able to directly help L. But they do need to be able to pass on the information to someone who can.

Learning check

A person goes to their GP for some routine care.

During their appointment, they tell their GP that they are thinking about kidnapping their children from their estranged ex-partner. The GP thinks this is more than just blowing off steam, and it's a serious threat.

WHO SHOULD THE GP TELL ABOUT THIS?

A. The Police
B. The pharmacist
C. The practice nurse.

The correct answer is A. The Police can take action to prevent this from happening.

Suspected abuse

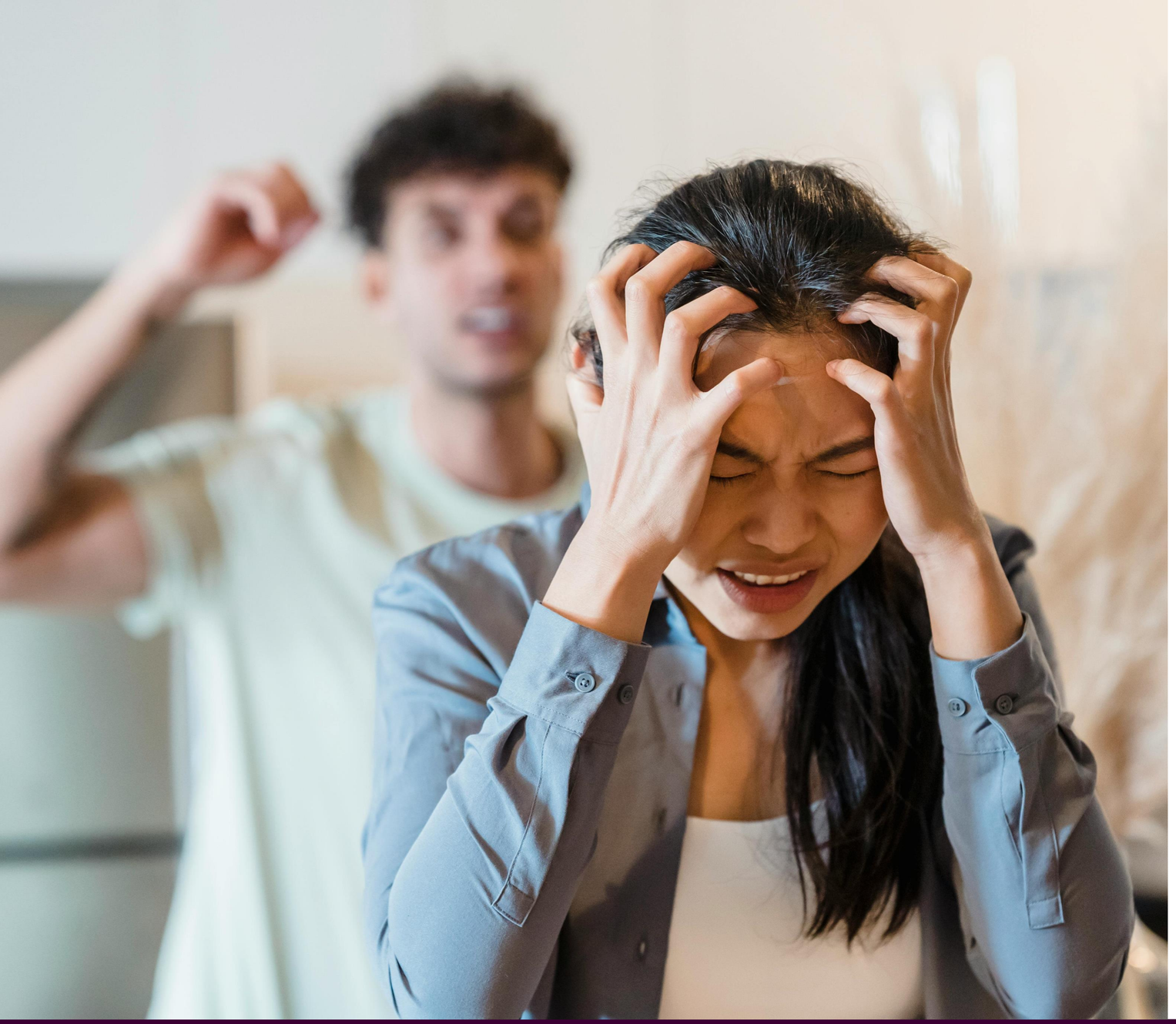
When you disclose information because you suspect there is a serious threat, you do not have to be correct. The information also does not have to be relevant - you just have to have a good reasons to think that it is relevant.

EXAMPLE

A Plunket nurse is doing an in-home visit for a new parent. They see some bruises on the newborn, and suspect the baby is being abused. The nurse calls Oranga Tamariki - Ministry for Children.

Oranga Tamariki launches an investigation, and finds that the child is being raised in a loving home, with no abuse. The bruises were from an accident.

The Plunket nurse will face no consequences. They thought there was a threat, so they disclosed the information they needed to disclose. They were still right to tell the Ministry and spark and investigation, even if that investigation did not ultimately find anything.



Learning check

A counsellor is seeing one of their clients. The client makes an offhand remark about abusing their partner when they get home.

The counsellor challenges them about this remark, and the client backtracks, and insists that they were just joking. The counsellor is not convinced. What can they do?

A. Tell someone, such as a Police officer.

B. Keep the information to themselves.

The correct answer is A. Since the counsellor thinks there is a serious threat to their client's partner, they can tell someone. Even if it turns out the client was joking, the counsellor will not be in breach of the Health Information Privacy Code.

When patients want to record you

This section explains what you can do when patients and patients' families record medical professionals.

Recording staff

Sometimes, patients may want to record health professionals. These circumstances are generally not covered by the Health Information Privacy Code, but you can still resolve them using other methods.

A private organisation, such as a GP's office, can require patients to not take pictures or videos as a condition of receiving services from that organisation.

This can be more difficult for public organisations, such as public hospitals. You are unlikely to deny patients chemotherapy for filming a nurse.

In general, it is better to approach situations on a case-by-case basis, rather than setting blanket rules.

One exception

In some cases, a patient might breach a health or disability professional's privacy.

This is limited to situations where the information collected would be 'highly offensive'. For example, recording a nurse as they use the bathroom would probably meet the 'highly offensive' threshold.

This also applies to the way a patient uses information. Recording something for personal use may not be highly offensive, but posting it all over the internet may be highly offensive.

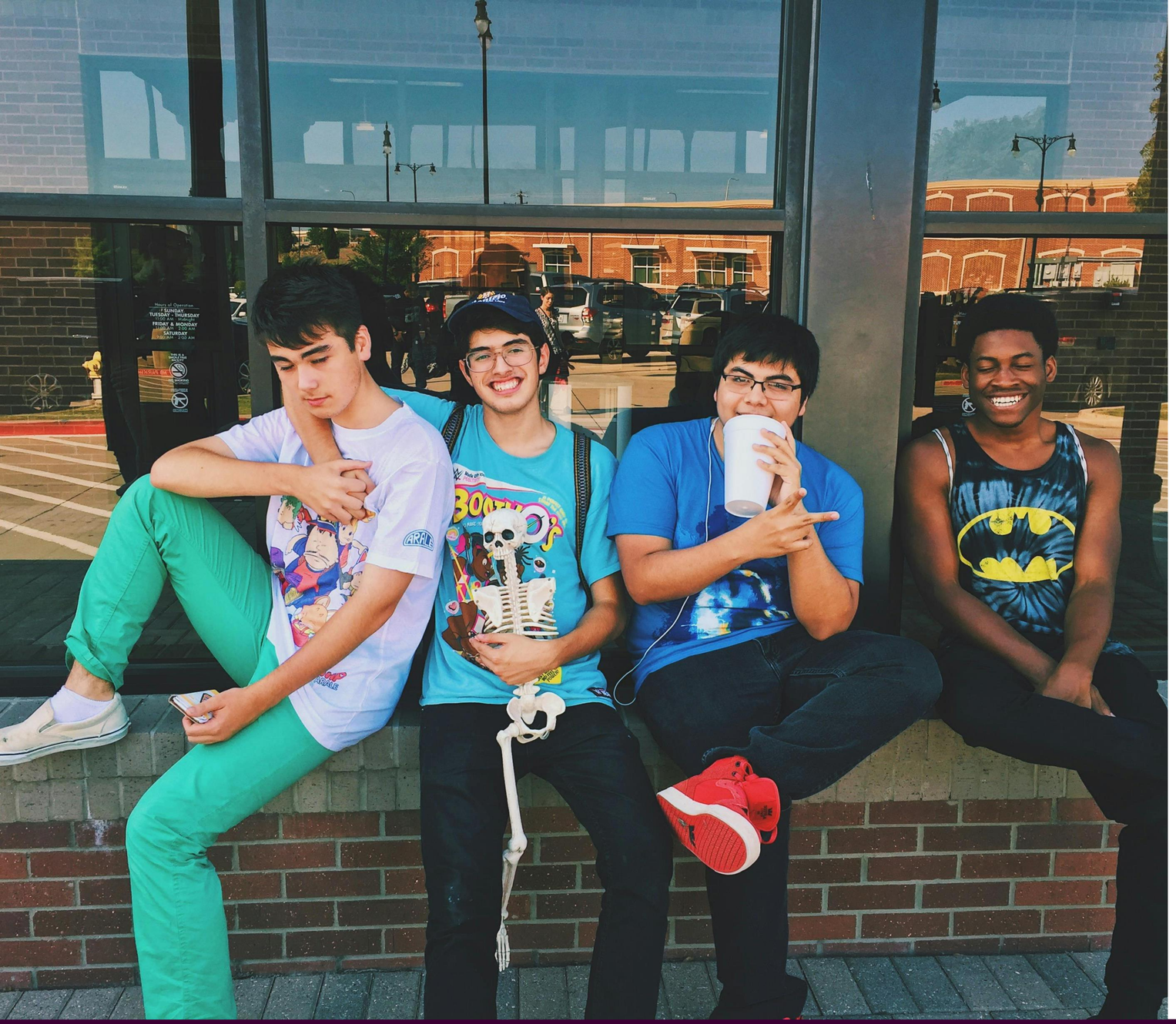
These are determined on a case-by-case basis. They do not come up very often.

Have a conversation

The best way to assess a situation where a patient is recording is to have a conversation.

You should try to find out:

1. What they want to record
2. Why they want to record it
3. How they will use the recording.

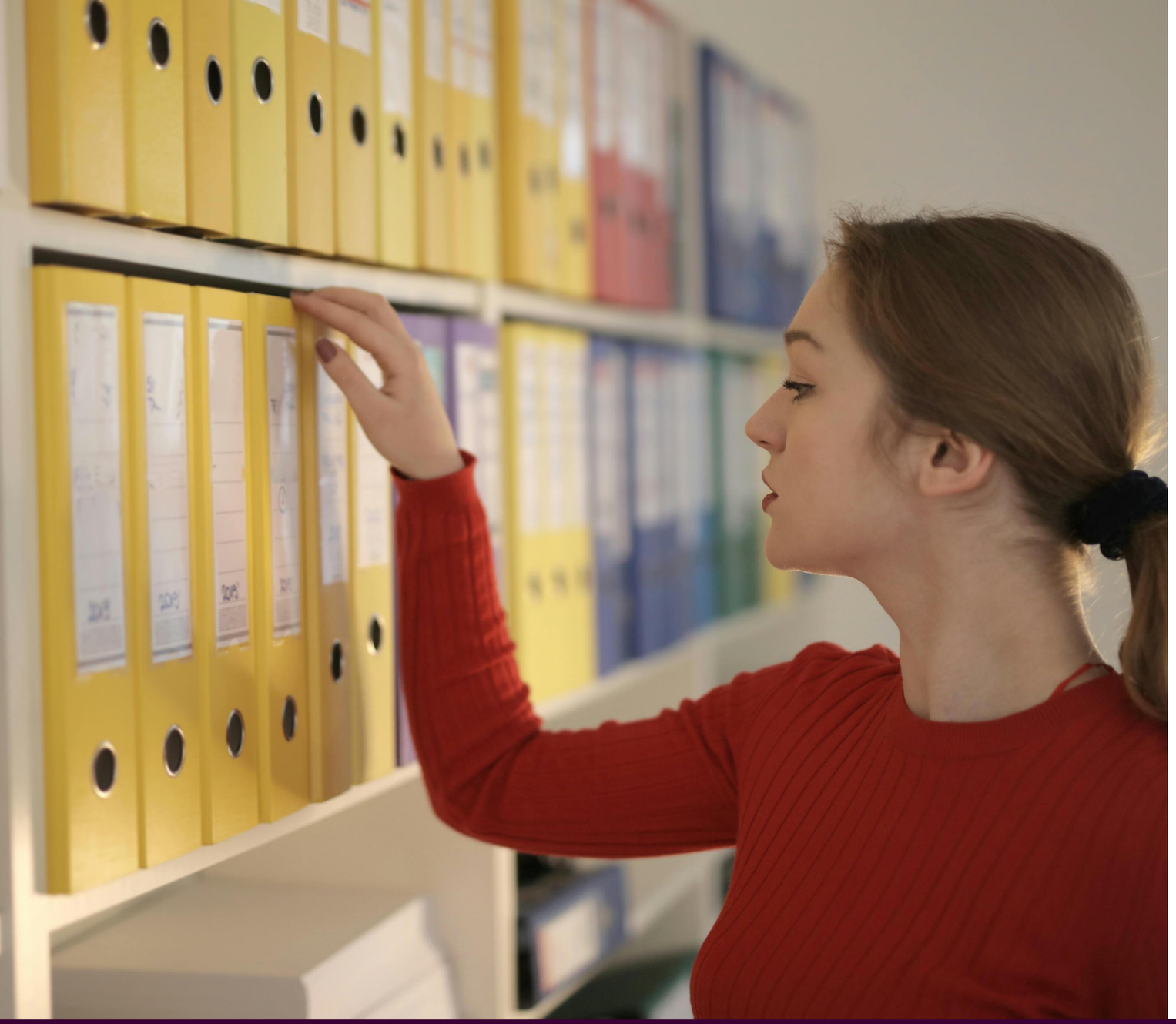


Teenagers in the ward

A teenager has cancer and needs to spend several weeks in the oncology ward. On their birthday, their friends visit and video them opening presents. A nurse is incidentally caught in the frame in the background.

The nurse tells the teenagers that they aren't comfortable being recorded.

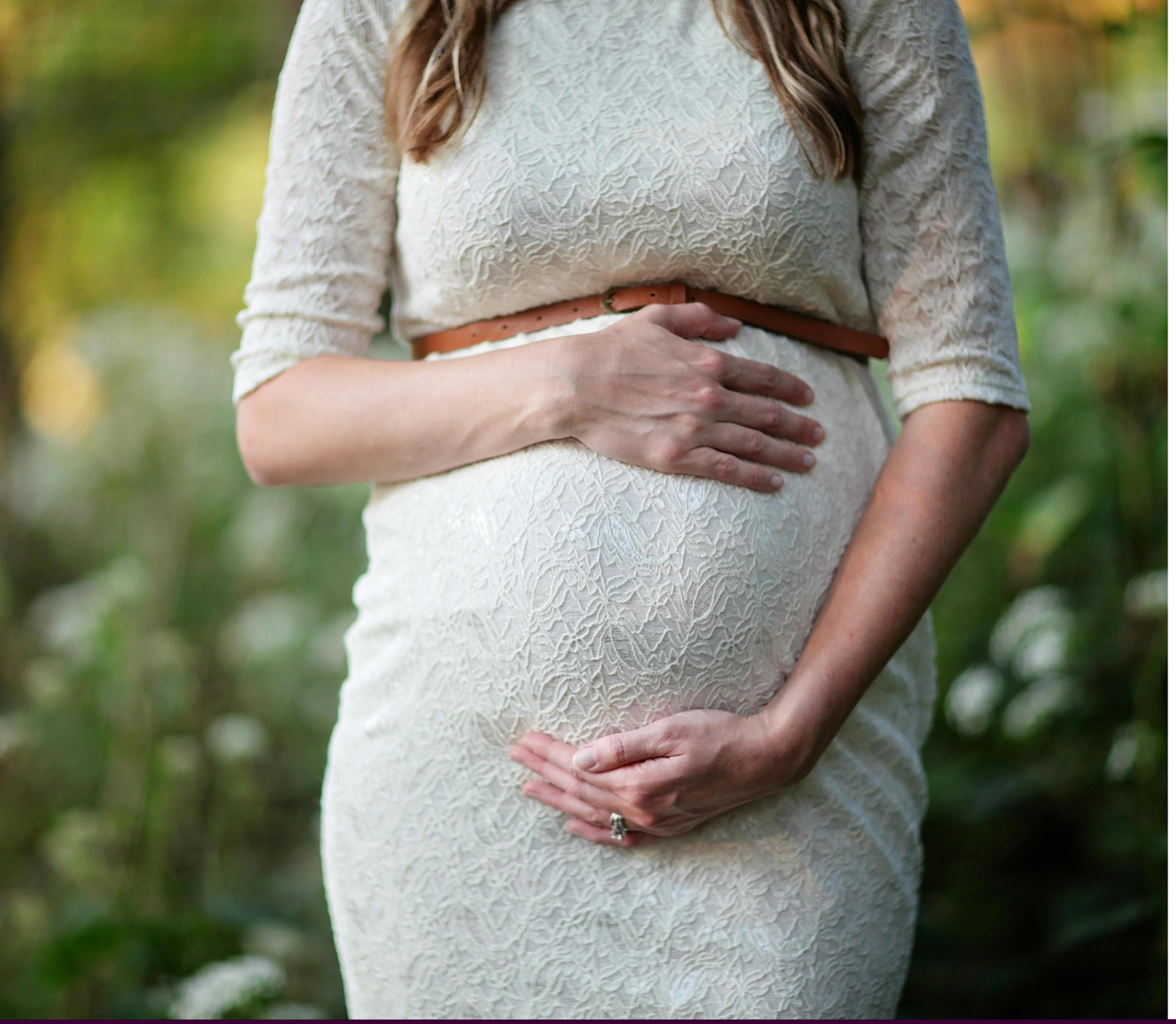
They show the nurse the footage, agree not to put it on social media, and agree to let staff know if they want to record anything in the ward in future.



Keeping personal records

A patient is seeing their GP. They have lot of questions, and want to make sure they remember the answers after the appointment is over.

They tell the GP they intend on recording the appointment on their phone for this reason. The GP agrees, but asks them to just record audio, not video. They agree to these terms.

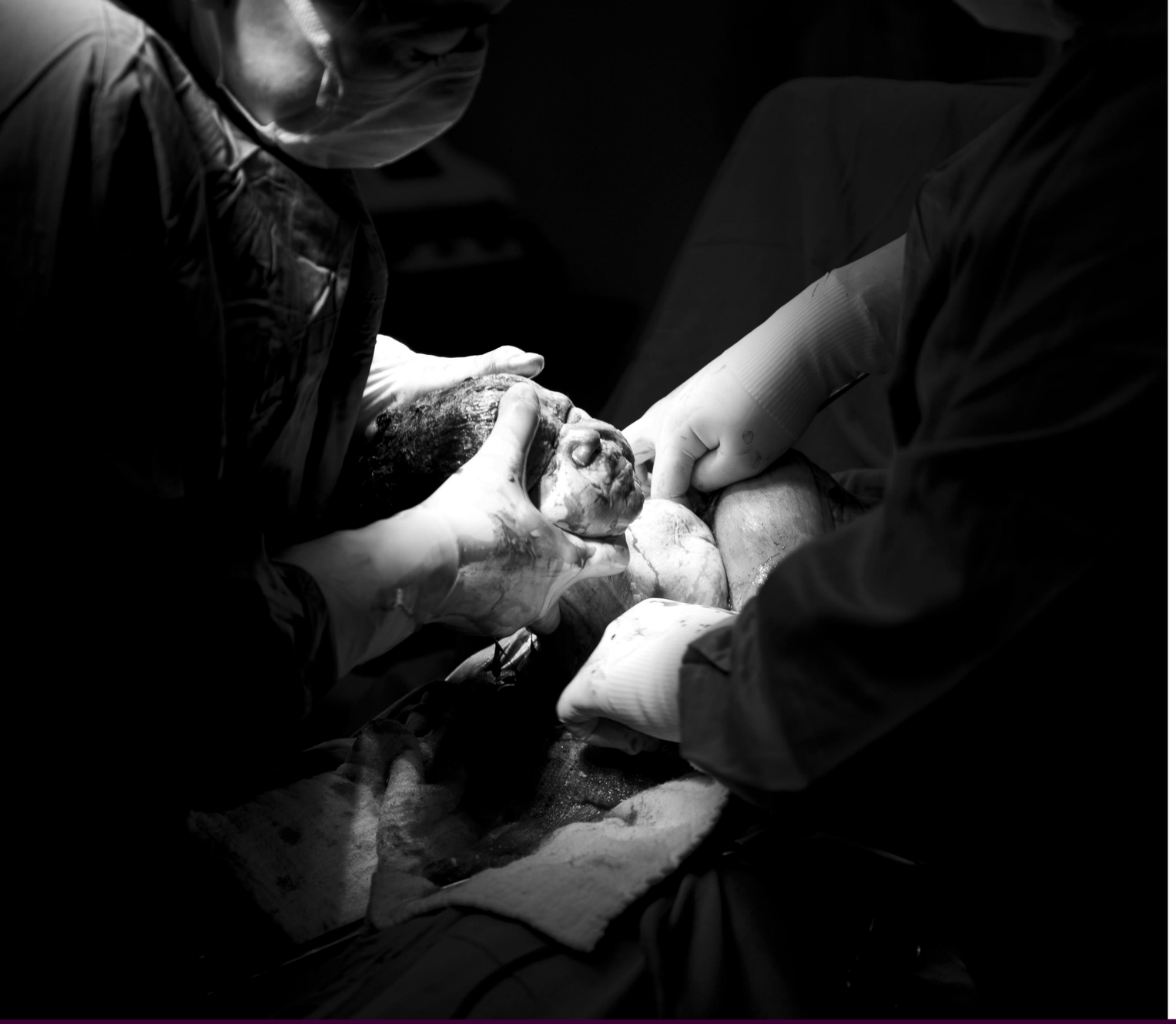


Relationship breakdown

The relationship between a midwife and their patient is breaking down. One day, the patient says that they will be recording all appointments from now on.

The midwife has allowed themselves to be recorded by patients in the past, but they are not comfortable with this patient recording them, due to the context of the relationship breakdown.

They tell the patient that they need to find a new midwife if they need want to record appointments.



Distractions in the ward

A woman is giving birth via caesarean section.

Her partner wants to capture this significant event, so is recording it with a Go-Pro style camera. The medical staff find this extremely distracting, and tell the partner to stop recording if they want to stay in the room.

There is no negotiation or discussion.

Summing up

There are a lot of different circumstances where a patient may want to record their interactions with a health or disability professional. Some of these may be fair, and some may not be.

The most useful strategy is to approach each situation on a case-by-case basis. You should make each decision based on the context of **what** the patient is recording, **why** they want to record, and **how** they will use the recording.

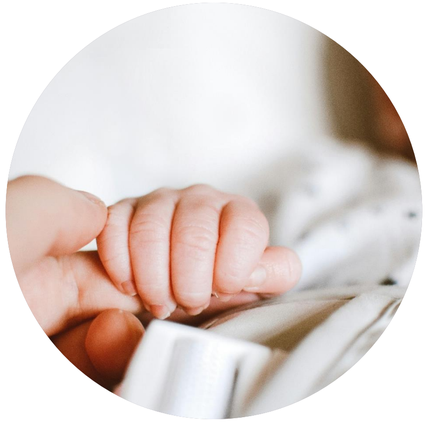
And remember: if someone records highly offensive content, or uses recorded content in a highly offensive way, you may be able to seek a remedy for this by making a privacy complaint about that person.

Working with children

This section covers what you need to consider when parents ask about their children's medical records.

Patient’s guardian

The Health Information Privacy Code allows medical information to be disclosed to a patient's guardian. In many cases, children's parents are their guardians as well.

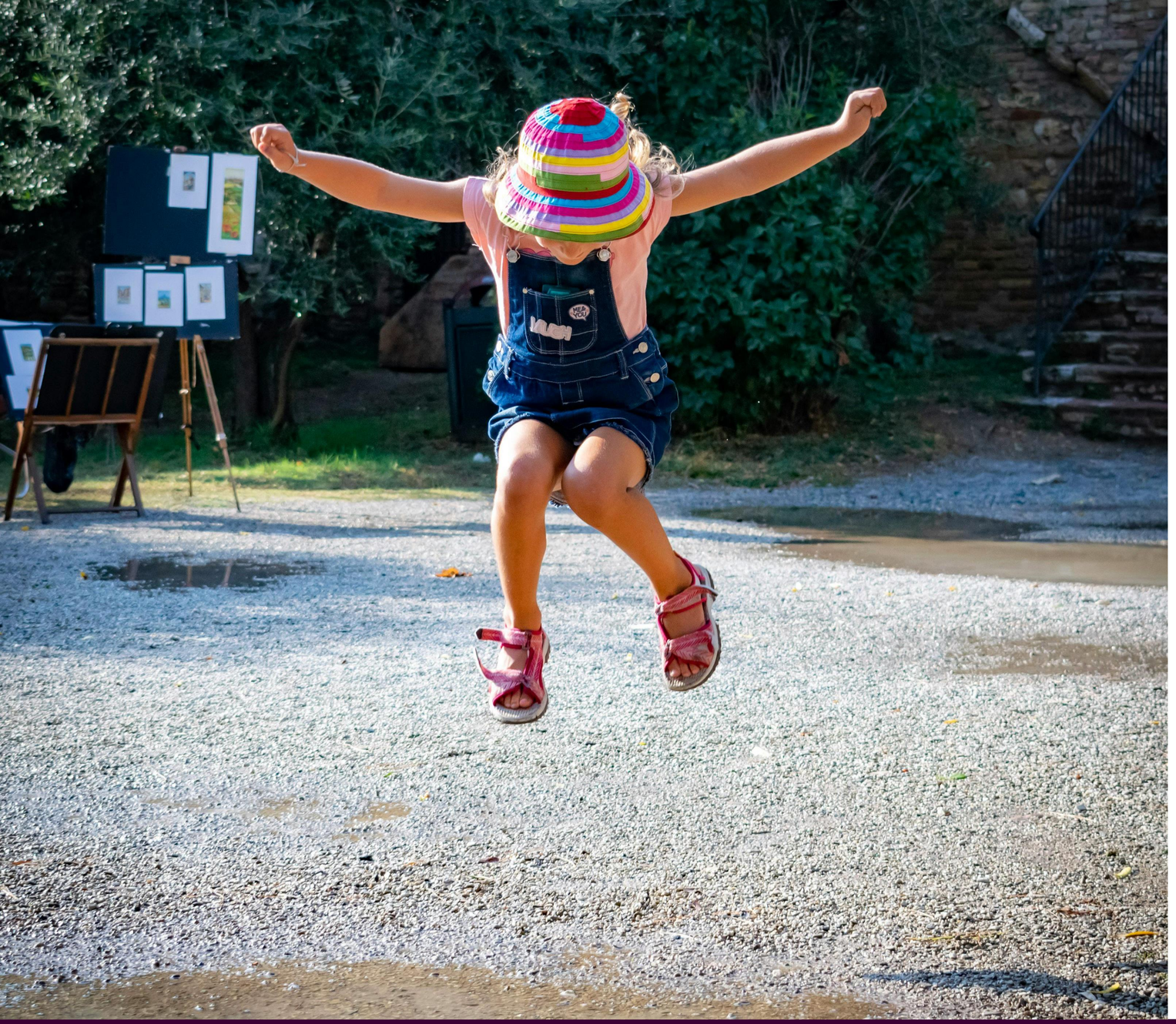


MEET R

R has a three year old child and needs some of their information from their GP to fill out a health insurance form. R calls the GP and asks for the information and the GP gives it to them.

This will usually be acceptable under the Health Information Privacy Code. Since R's child is only three, and her parent is her guardian, they have the right to see the child's information.

This usually applies to children and teenagers up to the age of 16.



Exceptions

Parents do not have a blanket right to see their children's information.

Health professionals can refuse to give information to a parent if they think that giving it would be contrary to the child's interests.

This decision is left to the health professional's judgement.

Learning check

R does not live with or get along with L, their child's other parent. L is also not a caregiver for their child. L has illegally taken their child in the past, and Police have been involved. As a result, L does not know where R and their child live.

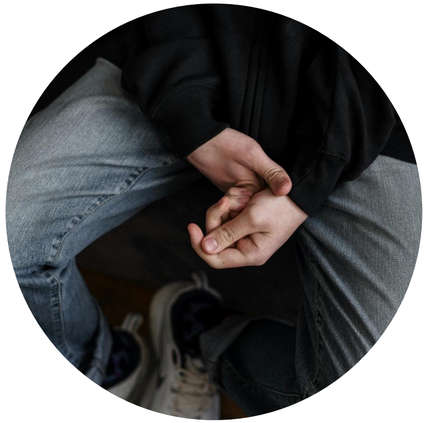
L calls their child's GP and asks for a copy of some test results. The test results have R's address on them. Does the GP have to give this information?

A. Yes - L is the child's parent.
B. No - L is not a guardian.
C. No - giving the information may not be in the child's best interests.

The correct answer is C. The GP needs to decide whether giving this information is in the child's best interests. They could decide that it's not in the child's interest and give L the test results. They could also give the test results without giving the child's address.

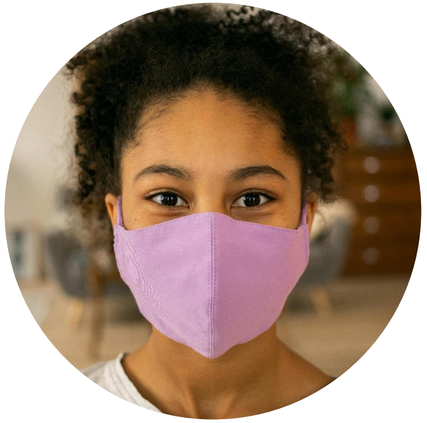
Patient’s interests

These situations are difficult, and they are ultimately up to the judgement of the person providing medical care.



A twelve year old is seeing a counsellor. Their parent asks to see the notes from the counselling sessions.

The counsellor may refuse to give these notes if they think that giving them to the child's parent would harm the child.



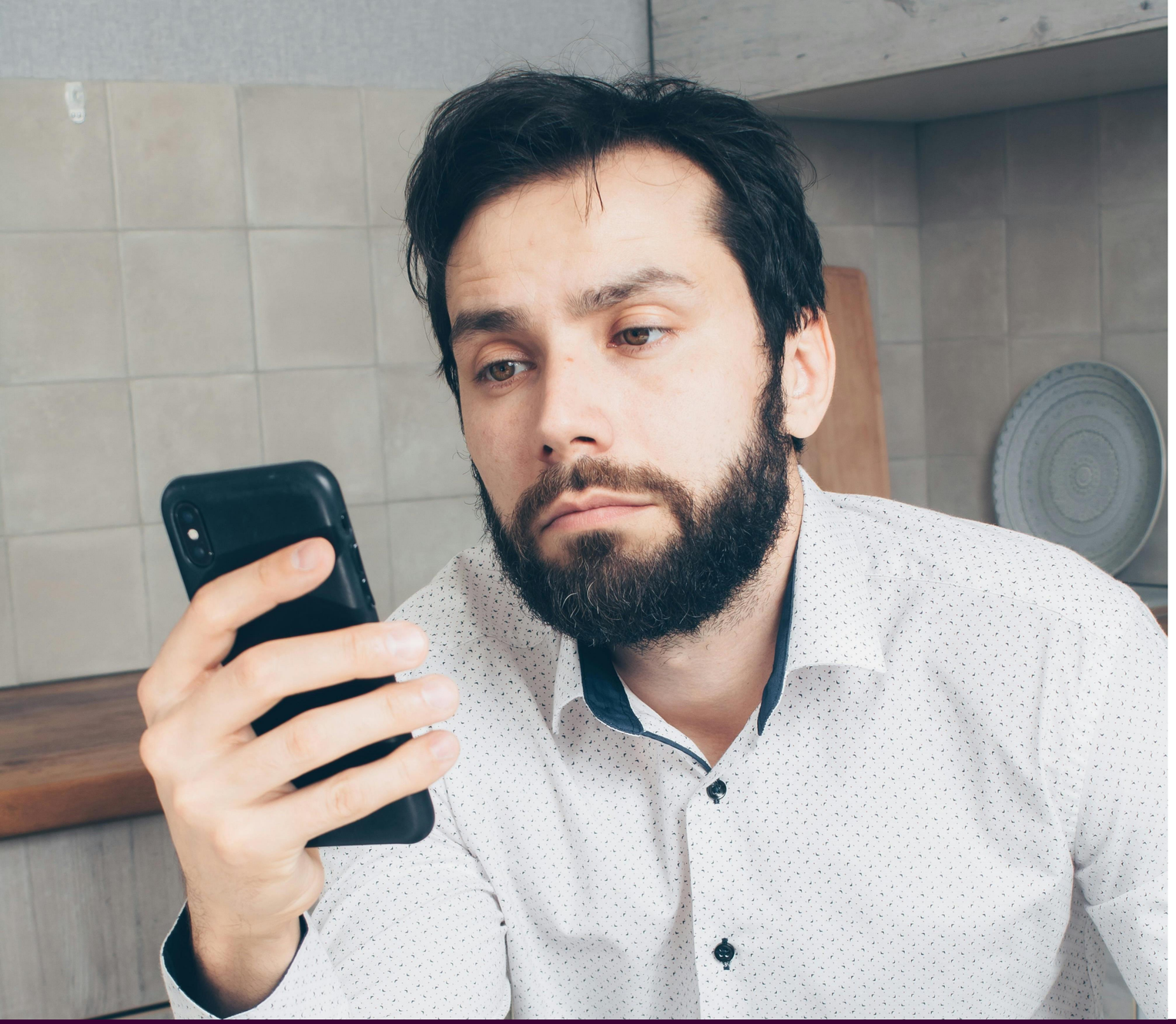
A 15 year old goes to their GP and asks to be put on birth control pills. The teen’s parent calls and asks the GP to tell them the details of the appointment.

The GP does not have to provide the teenager's parent with the information, but they also don't have to refuse to provide it. Telling the teen's parent would harm the trust between the GP and their patient, but there may be situations were this trade-off is worth making.

The GP needs to decide which option would be in the best interests of their patient.

Human error

This section focuses on how you can try and prevent human error from leading to privacy breaches.



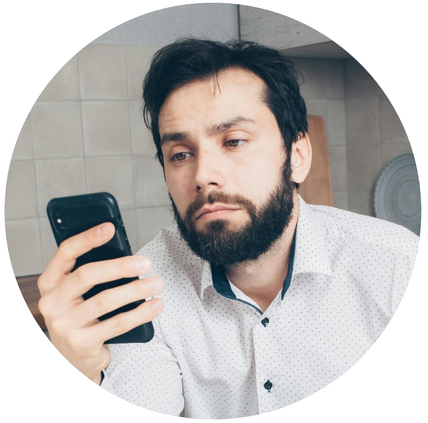
Human error

Human error is one of the biggest causes of privacy breaches.

If a patient whose privacy has been breached makes a complaint, your employer could be found to have interfered with the patient's privacy.

Changing systems

The big privacy breaches can happen in the small jobs.



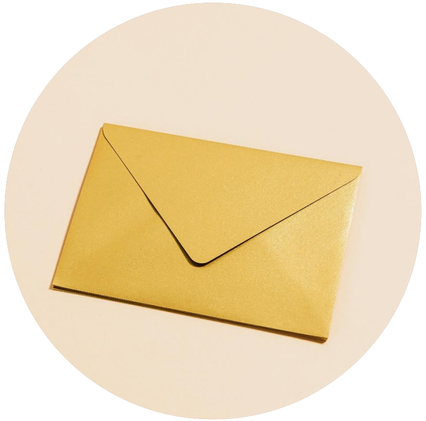
When you're doing a job that involves personal information, think about what kind of human error you could make - and what you can do to avoid it.

The best way to avoid human error is to change the systems and processes you use, rather than being 'extra careful.' This is a balancing act.

Too many safety checks, and you can't get anything done. Too few, and you risk breaching someone's privacy.

Meet J

J is a receptionist at a GP's office where part of their job is to send out letters to patients each day. They put the letter in an envelope, write the address, then post it.



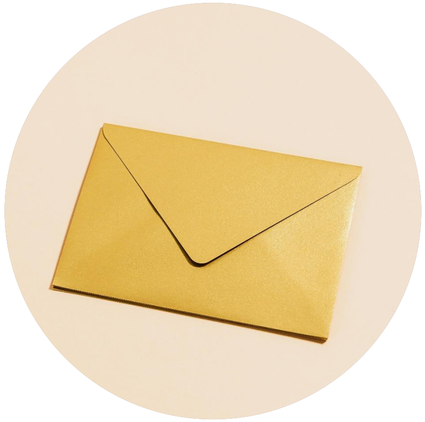
One day, J is distracted by a question from a colleague in the middle of this process, and they write the wrong address on an envelope. A patient gets a letter intended for another patient, containing the other person's sensitive medical information.

This is a privacy breach of sensitive information. There is a requirement to notify the Privacy Commissioner of privacy breaches that have caused, or may cause, serious harm.

Jo may need to alert the Privacy Commissioner, and may also need to inform the affected individuals. Jo can use the online tool NotifyUs to assess and report the breach.

Learning check

J decides to change the way they are going to send out letters in order to prevent a similar breach happening again.



Which is the best solution?

A. J switches to windowed envelopes, with the recipient's name and address on the letter itself.
B. J sends every letter via courier, with instructions to have each letter signed for by its recipients.
C. J puts letters into every envelope, but doesn't seal them, then checks each one before they seal it.

The correct answer is A. This solution is more reliable and easier than the other two options.

Taking information off site

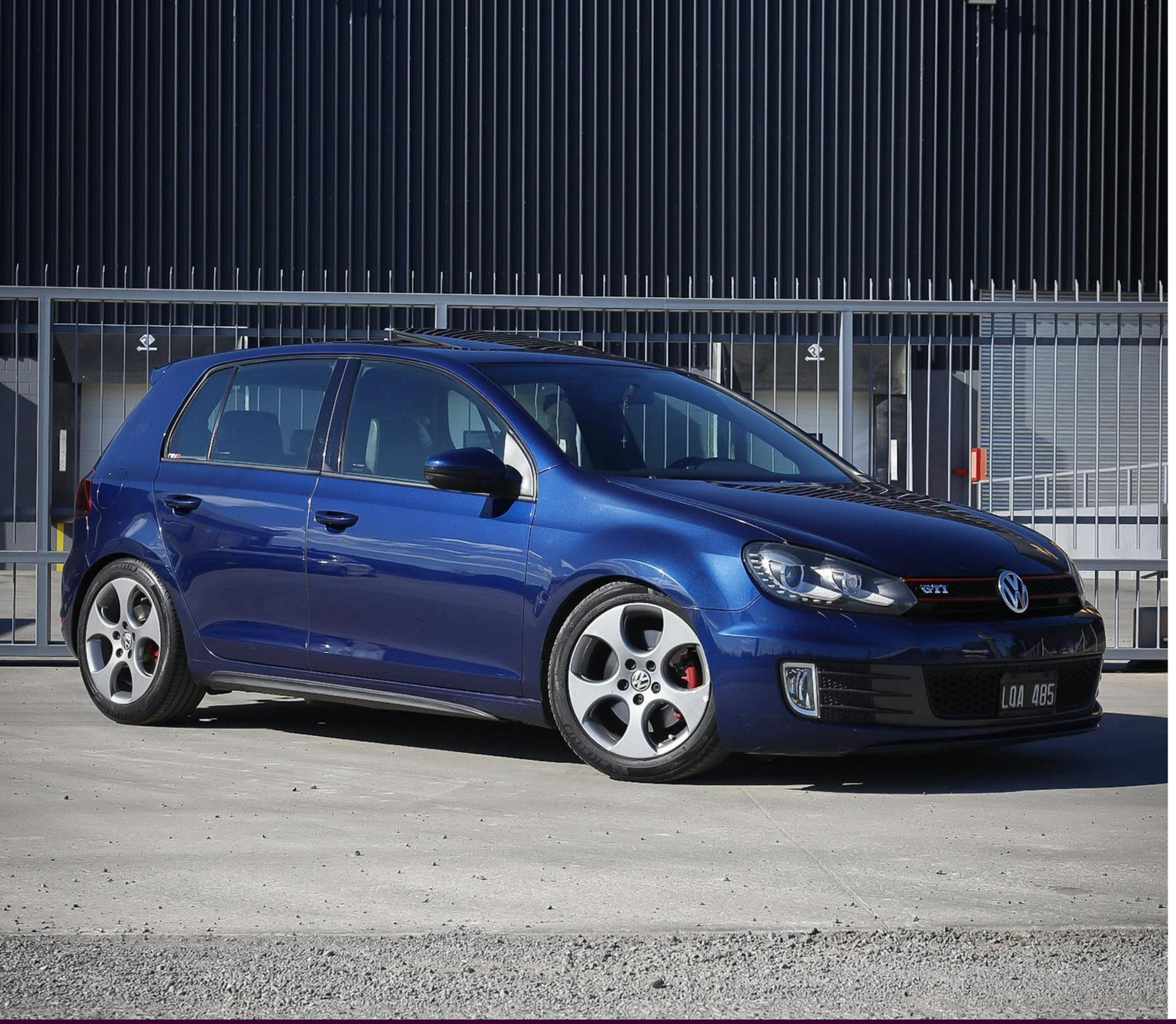
In this section you'll learn about the considerations involved when staff take patients' health information off site.

Rules of thumb

When you take information off site, you need to make sure you are only taking the information you need.

You also need to make sure you are protecting the information that you take. When you take information off site, remember this rule…

YOU CAN’T LOSE WHAT YOU DON’T HAVE, SO DON’T TAKE WHAT YOU DON’T NEED.



Meet D

D is a social worker for a hospital. They work in the community, visiting patients in their homes to check up on them.

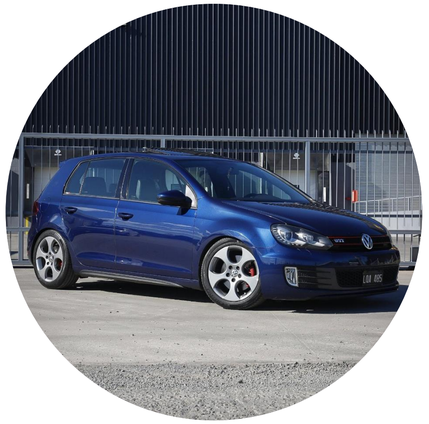
They leave to see a few patients, and load their car with a box full of patient files. Unfortunately, the car is stolen, and the box of patient files is never seen again.

This is a serious privacy breach, so the hospital needs to inform the Privacy Commissioner and may need to inform the people affected. D can use NotifyUs to do this.

D cannot control whether their car is stolen, but they can control what is in the car.

Learning check

How could D have managed this more effectively? Rank these three options from best option to worst option.



Which order should these go in?

A. D goes off site with a box of 100 files, even though they're only seeing 20 patients, to save them time finding only the files they need.
B. D goes off site with just the 20 files they need.
C. D loads electronic versions of the files on a password-protected laptop.

The correct order is C, B, then A.

Learning check

A junior doctor needs to prepare for their cases for the following day. They intend on doing some of this preparation from home.

Rate these three options from best privacy practice to worst privacy practice.

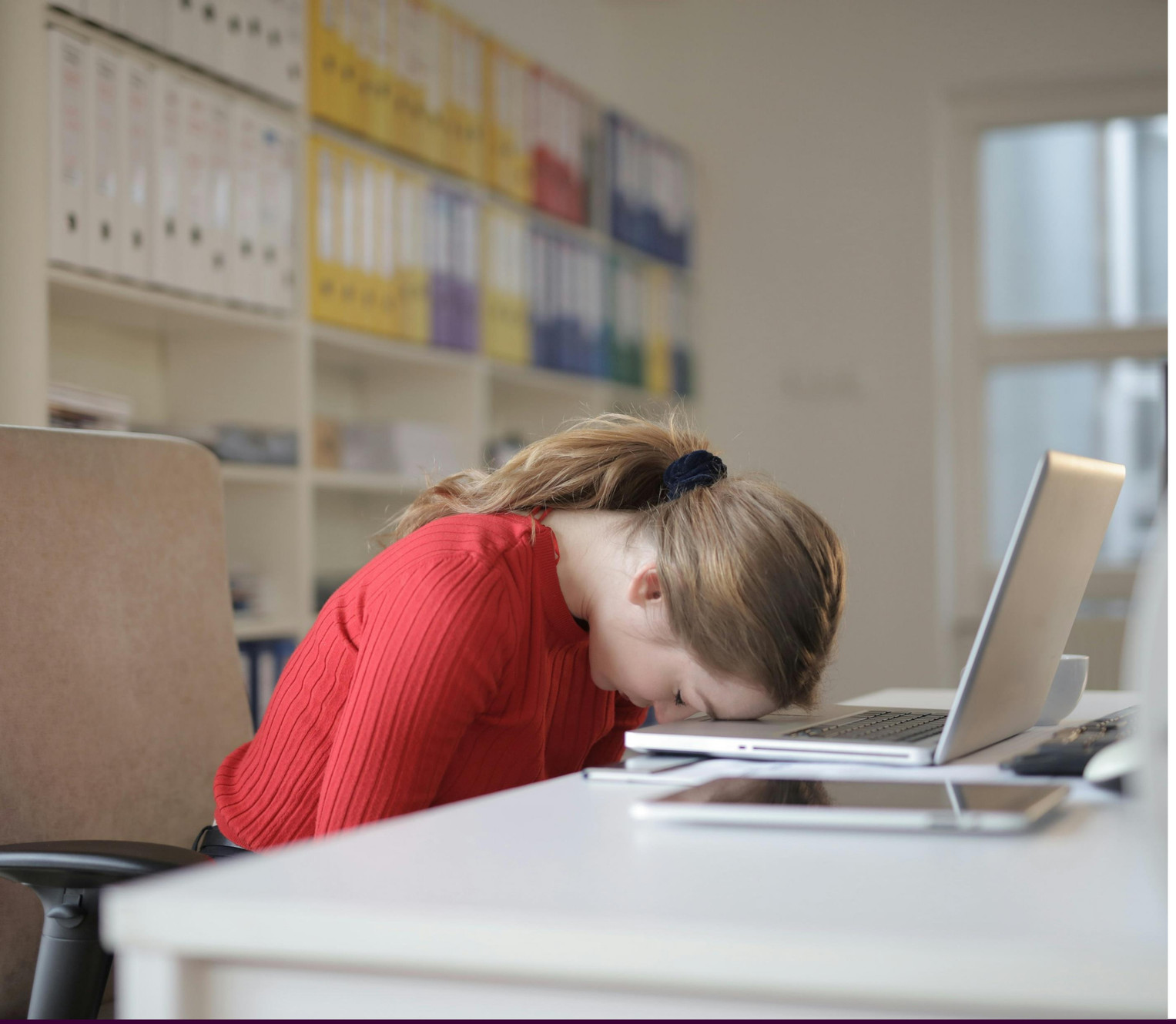
A. The doctor downloads the relevant files onto their laptop.
B. They print out the files they need and takes them home.
C. They log onto the system from home.

The correct order is C, A, B. Logging in from home is the best way to get information off site, because they have the hospital's security systems at their disposal.

Downloading the files on their laptop will work if they can't do this, but they could still get a computer virus. Printing out the files is the worst of these options, and should be avoided if possible.

Dealing with data breaches

This section looks at what questions to ask and what actions you should take when a data breach occurs.



Privacy breaches

Privacy breaches are when health information gets lost or sent to the wrong person, or when someone has unauthorised access to information. If they do happen, they should be carefully managed to reduce the harm they cause.

When you have a privacy breach that could cause serious harm to someone, you must tell the Privacy Commissioner and in most instances also the affected individuals.

There is more information about privacy breaches, including how to report them to the Privacy Commissioner at privacy.org.nz

Meet K

K works in administration for a public health trust that provides day-to-day living services for people with intellectual disabilities.

They have a spreadsheet with a list of 200 clients, their names, addresses, and level of care required (given as a number between 1 and 3). They need to send this to the Ministry of Health. They attach it to an email, and type in the address. Unfortunately, the auto-complete fills in the name of one of the trust's suppliers, not the contact at the Ministry of Health.

K sends the email without realising the error. K has inadvertently caused a privacy breach. To deal with it, they need to ask a couple of questions:

1. How many people have seen the information?
2. How can they contain the information?

K decides they can answer both of these questions by having a conversation with the supplier. They call the supplier, tell them what's happened, and ask them to delete the spreadsheet. The supplier tells them they hadn't opened the spreadsheet yet, deletes it, and the breach is over.

When to tell people

In K's case, they probably don't need to tell the 200 clients in the privacy breach. Nobody saw the information, and they quickly contained the breach.

When things go wrong, you may need to tell the Privacy Commissioner, and sometimes you will need to tell the people affected as well.

If the information has caused, or may cause, serious harm then you need to report the breach.

Use the online tool NotifyUs to assess the breach and report it if necessary. They may need to do something about it, and to do so, they need to know that there has been a privacy breach.

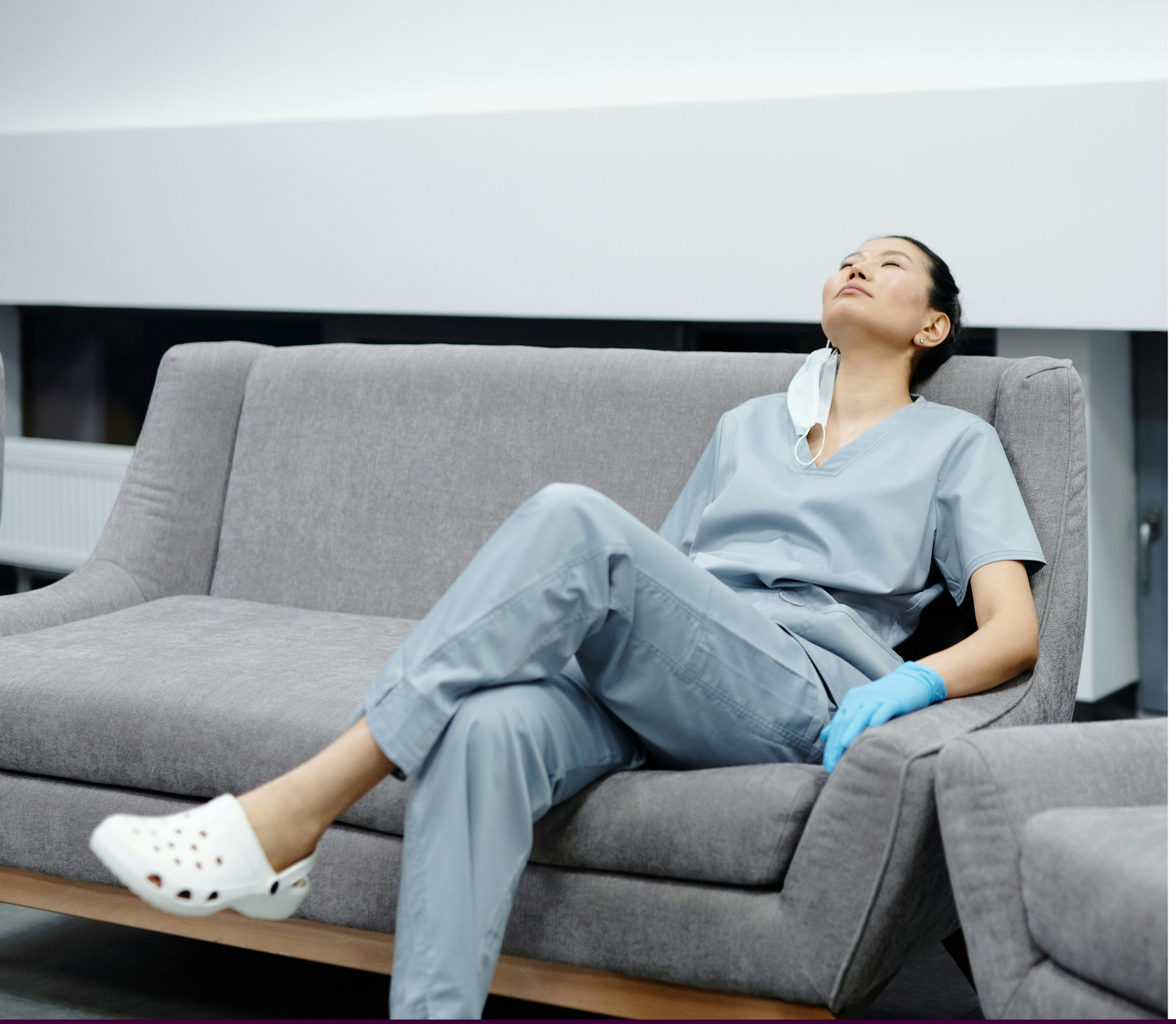
Meet N

N is a nurse for the local hospital.

They have a list of patients who have had gastric bypass surgery in the last few months, with their names, surgery details, and phone numbers. They use this list to call them and follow up on their outcomes.

N accidentally emails this list to one of the patients, and does not realise until the patient emails them back alerting them to the error.

They ask the patient to detail the information, but the patient refuses.



Two questions

If N runs through the same questions K ran through, it doesn't look very good.

1. How many people have seen the information? At least one person, and possibly more, as the patient may share it.

2. How can I contain the information? N cannot contain the information, although they have tried their best.

With these two things in mind, N decides to alert their supervisor, the patients, and the Privacy Commissioner.

They use NotifyUs to do this.

Learning check

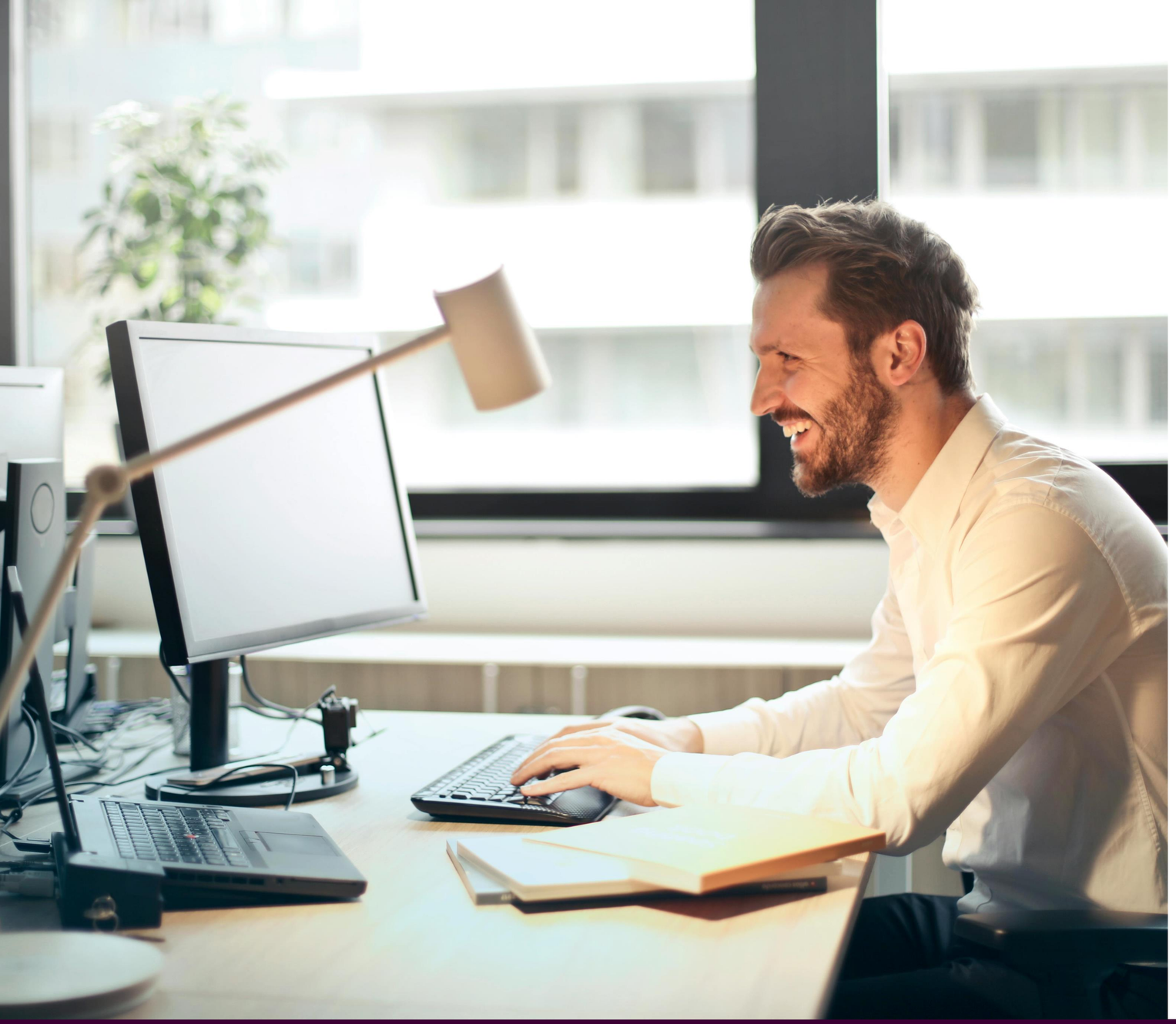
Should the organisation tell the people concerned that there has been a privacy breach in these scenarios?

1. A notebook full of patient notes is left in the back of a taxi, and is never seen again.

The correct answer is yes. It's unclear how many people have seen the information, and the agency cannot do anything to stop the information from spreading further, so it should tell the Privacy Commissioner and the patients concerned so they can take any action they need to protect themselves.

2. An encrypted USB full of sensitive insurance claim data falls out of a private hospital worker's pocket in a cafe.

The correct answer is no. It's probably not necessary. Nobody will be able to see the information, and the fact that the USB is encrypted has automatically stopped it from spreading further.



Learning check

Should the organisation tell these people that there has been a privacy breach?

A GP's office sends a letter to the wrong patient.

The practice manager calls the patient who received the letter, but they cannot contact them.

Yes. The subject of the letter should probably be notified, because at least one person may see the information, and the GP's office cannot guarantee that the breach is contained.

Congratulations!

You’re at the end of Health ABC. You can also do this as an e-learning module online at privacy.org.nz anytime for free.

Privacy Commissioner
Te Mana Mātāpono Matatapu