we are withyou

Privacy, Sharing and Confidentiality Policy

Overview

What is this policy?

This policy is about how and when we share people's personal data so that our services are effective and safe. It sets out what we do with the data that we have (such as information about the people who work for us and who use our services).

It's published on our website so anyone can see it, and it applies to everyone - people who work for us and people who use our services.

Guidance about how the people who work for us should act is in the blue 'Resources' boxes throughout this document, that only they can access.

When do we use this policy?

Use this policy before using or sharing any information and data. If you think data has been mishandled or shared inappropriately, this policy will tell you how we expect the people who work for us to act.

Use this policy with our other policies about how we look after information: Data Security and Protection policy and Information Rights policy. You can find them on our website, or if you work for us, you can access them through our shared drives.

What's included in this policy?

This policy was last updated: July 2022

This policy will next be updated: July 2023

This is a controlled document, do not print or make a copy.

What are Privacy, Sharing and Confidentiality?

Privacy

We all have a right to expect respect for our private and family life under the Human Rights Act (and United Nations Convention on the Rights of the Child (UNCRC) if you are under 18). That means that you have the right to keep some things - like your body, identity, relationships and your personal information - to yourself, and choose what is shared with others and when. Other laws give you specific rights about your data (see our Information Rights policy).

We all have a duty to respect other people's rights and freedoms. The right to privacy is known as a "qualified right". That means to be fair to everyone we must think about the community's rights as well as everyone's individual rights.

Confidentiality

When you share information with us, we keep it to ourselves. We know that you trust us with your personal information. Confidentiality means that we will keep it safe (our Data Security and Protection policy tells you how we do this) and not tell others unless:

- You say it's ok to share it (you give your consent)
- It stays inside We Are With You
- There's no way of telling it's you from the data (like in a report)
- Someone might get hurt if we don't share it
- A court orders us to
- It's a certain health condition that we have to report (like Hepatitis B cases)

Sharing

Sharing data happens whenever someone gives or gets information from another place. This might be by listening to, reading or seeing something or someone. Sharing is how we learn about people and things so we can make decisions. In our work, we think sharing information is really important so that we can:

- Understand what's going on
- Achieve the goals we've made together
- Keep you and others safe
- Make our services better for everyone (like when we do an audit of our

services)
- Tell others about the work we do

We make sure we only share what we need to do our jobs properly. So if we can use reports where we can't identify anyone, we will.

→ Further reading: Privacy, confidentiality and sharing (links to other sites)

- Human Rights Act 1998 (Article 8)
- United Nations Convention on the Rights of the Child (UNCRC) 1990 (Article 16)
- Data Protection Act 2018 (DPA)
- We Are With You's online confidentiality statement and privacy commitment
- Caldicott principles on using and sharing information

Giving consent

Be as open as you can

We think that being open and honest is really important. It means that we have all the facts and can make good decisions with our service users about their care. We know that involving friends and family can make a real difference to someone's journey with us. Linking up with different types of services helps to support people beyond what we can do on our own.

We always ask who we can share information with when we start working together, and keep checking regularly to see if anything's changed. We might do this on paper (for example using a consent form, which we then upload to our database), or by making a note on the record (if we met by telephone or video). If we think someone can help with a research project or media campaign, we'll explain it and ask for consent for it specifically.

Make sure consent means something

We ask for consent if we're sure the person knows what it really means and that it is an actual choice (where your choice doesn't affect the service you get). The

people who work for us are trained to take into account "capacity or competency to consent". It wouldn't be fair to you if we held you to decisions that you couldn't understand.

We use well-respected tools and guidelines if we think someone may need help understanding their treatment or consent to sharing. We can then involve others to help us make decisions together about their care.

If you are a child (aged under 18 in England or under 16 in Scotland by law) we take extra care to make sure you know what is going on and can give your consent, while respecting your privacy and confidentiality. This might mean we work together and get the support of a person who is responsible for looking after you.

→ Resources: Giving Consent

- How to....Write a great privacy notice
- How to...Look after audio and video recordings (links to consent forms for media and audio and video recordings)
- How to....Share information safely
- WhatsApp Group (consent form)
- Safeguarding elearning - Adults, Children and Information (on Looop)
- Gillick competency and Fraser guidelines
- Mental Capacity Act training (on Looop)

If you need further help, email us at data.protection@wearewithyou.org.uk

When we share information

So that we can work together

If we need to share information with another professional so that we can start

working together (like telling your doctor before we start prescribing), we make sure that it's clear when we talk and that it's written on the service's privacy notice. That way we can discuss any questions at the start and the person can choose whether to go ahead with that type of support

If we're worried about your safety

There are times when we need to share even if you haven't told us what you want us to do or you've said you don't want us to. We sometimes call this "breaking confidentiality" and we'll only do it if we have a good reason. We'll tell you what we're going to do, unless we think that would make the situation worse or we can't for practical reasons (like if you were reported missing and we shared information to help find you).

To keep the team informed

When we work together, usually you'll mostly see one person (like a worker or therapist or line manager). Behind that person is a whole team working together across the country to support you and keep We Are With You running smoothly. The whole team is responsible for your care and trained to keep your data safe (find out how in our Data Security and Protection policy) and confidential.

We understand that it can be frustrating and painful when you have to keep telling your story over and over, so we share what people in the team need to know so you don't have to.

If there's someone you know personally in the team, let us know and we can help to make sure they stay out of your care. We trust the people who work for us to follow our code of conduct, policies and their training at all times, including online. If they haven't, we look into the situation and take action.

To help others

We make sure any useful information that isn't confidential is available to everyone so that people can get help and support as and when they want it. We have policies and guidance about answering requests from the media and people who come into contact with our services. We update our website with information and tools that people can use to get support.

Some of our services share limited information to help understand what's happening around the country. We make sure we tell people about this in the service's privacy notice and our Your Data & Information leaflet (there are England, Scotland and Mental Health versions), as well as in our sessions.

If something goes wrong when data is shared

We understand that sometimes people make mistakes. We take extra care when we share personal or sensitive information by following our policies and guidance. But if something does go wrong, we will be open and honest with the people involved, and record it as an incident so that we can learn from it as an organisation.

NHS National Data Opt Out

The NHS sometimes shares Confidential Patient Information (CPI) for reasons beyond direct care, like for research or planning. The NHS National Data Opt-Out policy lets patients (that's everybody with an NHS number) in England choose if identifiable data from their health records is used for research and planning.

We Are With You does not use service users' CPI (that is data that identifies a person AND contains information about their health or treatment) for anything other than their direct care and treatment and we always ask the person first (getting consent), so the NHS National Data Opt-Out doesn't apply to us.

However, as an organisation we need to acknowledge these NHS provisions, so our staff are informed and can help service users if they have any questions, or if they need help opting out, following the NHS guidelines on how to make your choice.

In Scotland, the Scottish Primary Care Information Resource (SPIRE) requires patients wanting to opt out to complete a form and hand it to their GPs.

→ Resources: When we share information

- Data Security and Protection policy
- How to...Share information safely
- How to...Understand the Caldicott principles
- Staff Code of Conduct (DQ031)
- Disciplinary Policy and SOP (DQ008)
- Social Media Policy (DQ124)
- Download and print the Your Data & Information leaflet

(England, Scotland and Mental Health versions) through our Brand Centre

- Set an NHS national data opt out: https://www.nhs.uk/your-nhs-data-matters/
- Incident Management Policy (DQ199) and SOP (DQ199.1)
- Being Open and Duty of Candour policy (DQ197)

If you need further advice, email data.protection@wearewithyou.org.uk

Think before you share

Make sure it's covered in an agreement or contract

When we know we are going to share people's personal data with another organisation or service, we set up an agreement which says what, why and how we will share data with them. This agreement is generally an Information Sharing Agreement (ISA), which also may contain a data sharing protocol.

If working with the NHS, they often prefer to draw a Memorandum of Understanding (MoU), which may or may not contain a section dealing with data protection and sharing of personal data.

We keep track of these by adding them to a central log after they are approved and signed by the Data Protection Officer (DPO). Please contact the IG team for advice and help.

Check that you're only sharing what's needed

We always try to share the right amount of information - enough to do the job, but not more than is needed. If we can, we use data that's been mixed up and summarised (aggregated), had personal details removed (anonymised) or replaced with "random" IDs (pseudonymised) instead of data that would identify someone.

Before we share large amounts of data (like if we are closing a service and transferring data to the new provider), the person sending the information completes a "Stop and Check" with a Data team member. This is an extra check

to make sure we know where the information is going, how it's being sent, what's going to happen to it and what safeguards are in place to protect it.

Resources: Think before you share

- How to...Share information safely
- Information Sharing Agreement (ISA) template
- How to...Use the Stop and Check process (before sharing information)

Your privacy matters to us

Having a privacy mindset

If we think something we're about to start or change we are thinking of making might affect your privacy, managers do a Data Protection Impact Assessment (DPIA) - also called a Privacy Impact Assessment. A DPIA helps us think through all the benefits and risks to that project so we can decide how we can manage the risks and if it is worth going ahead.

Picture and sound recordings

We think hard before we use CCTV in our buildings. We know it can be really off putting for you, as well as being more work for us to set up and maintain. If we do need to use CCTV, we'll put up clear signs so you know it's there and can contact us. If we can, we'll use a live stream instead of recording the footage.

In a couple of our services, trainees might need to record some sessions for their course. We'll only record sessions if everyone involved knows about it and says we can. We'll use encrypted recording devices and only keep it for as long as we need (usually 12 months for video and 18 months for sound). We don't let anyone (whether they work for us or not) use their personal device to record sessions.

If we want to use pictures or video of you, like in a media campaign, we ask for your specific consent first. We delete it from our databases after we've finished using it. If it's used on social media (like Facebook or Twitter) or published in a news article or website, it goes into the "public domain". You'd need to ask the people who have used it to delete it, not We Are With You. This is one of your information rights.

Resources: Your privacy matters to us

- How to complete a DPIA (DQ402.5)
- Template Data Protection Impact Assessment (DPIA)
- How to...Look after audio and video recordings
- CCTV Impact Assessment
- Consent form for audio and video recordings
- Media Consent Form available from the Communications team
- How to...Archiving and retention
- How to...Look after records
- Information Rights policy

Policy version history	
Policy Title	Privacy, Sharing and Confidentiality Policy
Policy Number	DQ403
Version Number	1.2
Date of Issue	July 2022
Date of Review	July 2023
Sponsor	Company Secretary

Issue	**Page(s)**	**Issue Date**	**Additions/Alterations**
1	12	Sept 2020	New policy simplifying and replacing existing IG policies.

1.1	12	May 2021	Change of sponsor to Company Secretary
1.2	11	July 2022	Reference to NHS National Data Opt Out Policy