Staff Guidance on Individual's Rights under GDPR

Background

The General Data Protection Regulation (GDPR) provides individuals with the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

This guide has been developed to explain what these rights mean to care provider organisations and their staff.

General rules when dealing with individual's rights

1. When an individual makes a request, they can do so:
    a. verbally, in writing (hardcopy or digital) and even via social media;
    b. to any member of staff.

    As requests can be made to anyone, not just a specific member of staff or contact point, it is vital that all staff who might be asked are trained on what to do if someone requests their data from them.
2. You should have a clear procedure and keep a record of all requests and their outcomes.
3. You must respond to requests without delay and, at most, within one month of the request being made.
4. Sometimes, you might need to confirm someone's identity to respond to a request. You must ask them for ID as proof as soon as possible. Your time to respond to the request starts as soon as they provide proof of their identity.

5. You can have a two-month extension if the request is complex or you have received multiple requests from the individual. You must inform the individual why you need this extension within the first month.
6. Normally, you can't charge people a fee when they make a reasonable request.
7. You can charge a reasonable fee based on your admin costs if someone makes a request which is "manifestly unfounded or excessive" or if you need to make further copies of someone's data.
8. If a request is "manifestly unfounded or excessive" you can refuse to comply with the request instead of asking for a fee.
9. If you refuse a request, need to charge a fee, or require further information you need to tell the individual as soon as possible and at least within one month:
    a. why you are refusing the request;
    b. that they can complain to the Information Commissioner's Office (ICO[1]); and
    c. that they can seek to enforce their rights through a "judicial remedy" i.e. through the courts.

The right to be informed

All individuals have the right to be told about how their personal data is collected and used. You need to provide the people who use your services, your staff, and anyone else whose data you collect with information about:

- What information you hold;
- Why you have it;
- How long you keep it;
- Who you share it with; and
- Other information – a full list can be found here.

You need to provide them with this information in clear and easy to understand language in whatever format makes most sense for your organisation, i.e. online, in leaflets, etc.

You need to provide people with this information when you collect their personal data, e.g. you tell them why you need their information when they are filling in their admission forms.

[1] The ICO are the regulatory body for data protection. Not CQC.

Please note our disclaimer: https://www.careprovideralliance.org.uk/disclaimer.html

If you receive information about the individual from someone else, you need to provide that individual with privacy information within a reasonable period and at least within one month.

There is more information on how to provide this privacy information in our documents How to Document your Data Processing and Privacy Notice Template.

The right of access

People have the right to access *their own* personal data. Note that this right does not allow other people to request an individual's data, even if they are related to the individual, unless they have lasting power of attorney or some other written authority to make the request i.e. they are a lawyer acting on their behalf.

When people ask to have access to their own information, this is called a *Subject Access Request* or *SAR*[2]. We have an example procedure for SARs within our Record Keeping Policy.

When people make a SAR, they are entitled to:

1. confirmation that you have their data;
2. a copy of their data; and
3. the information which you would provide in a privacy notice (see 'right to be informed' above.)

There is more information on the ICO's website.

The right to rectification

Sensibly, individuals have the right to have their information corrected if it is inaccurate or incomplete.

If someone makes a request to have their information rectified, you should

- record the request;
- assess the accuracy of the original information and if it needs to be corrected or completed;

[2] Note, that they do not need to use the phrase 'subject access request'.

- if applicable, correct the mistake. You should keep a clear audit trail of corrected mistakes;
- regardless of outcome, you must let the individual know what decision you have reached.

There is more information on the ICO's website.

The right to erasure

This is also called the 'Right to be Forgotten'.

It is important to remember that this right **only** applies in specific situations. This is why it is so important to be clear on why you are processing data and your legal basis for doing so.

This right applies when:

1. you use *consent* for your lawful basis for holding data and the individual withdraws their consent;[3]
2. you no longer need the data for the purpose you collected it for;
3. you use *legitimate interests* as your lawful basis for holding data, the individual objects, and there is no overriding legitimate interest to continue this processing;
4. you are processing the personal data for direct marketing purposes and the individual objects;
5. you have processed the personal data unlawfully; or
6. you have to do it to comply with a legal obligation.

If you have disclosed their data to others, or the data has been made public, you must make reasonable steps to tell the other people using the data to erase it.

There are certain instances when the right to erasure does not apply. For social care providers the main ones are:

1. when processing is necessary to comply with a legal obligation;
2. when processing is necessary for public health purposes in the public interest (i.e. Article 9(2)(g));
3. when processing is necessary for the provision of health or social care (i.e. Article 9(2)(h)).

[3] This is one of the reasons why you should not be using consent for your basis for processing health and care data under GDPR

The last one is the most important. If you need their data in order to be able to provide care, you do not need to erase it.
When you comply with an individual's request to have their data erased, you must think of anything you have in back-ups or archives and make sure that this is also destroyed.
There is more information on the ICO's website.

The right to restrict processing

When you are asked to "restrict processing" this means that you can still store the data but you can't do anything else with it.

The right to restrict processing will often happen in conjunction with the other rights for example:

1. If someone is concerned that the data you have about them is inaccurate, they might also ask that you restrict processing while you investigate their request;
2. If someone objects to you processing their data, they might also ask that you restrict processing while you investigate their request.

You might also have to restrict processing when:

1. The data has been unlawfully processed but the individual does not want you to erase their data;
2. You don't need the data anymore but the individual needs it to "establish, exercise or defend a legal claim".

You need to think about how you will restrict processing in your organisation and have a clear procedure for what you will do. The easiest way of doing this will depend on how you keep information.

For example, if you mainly have paper records it might be easiest to remove the specific record and store it separately, in a locked drawer or similar, for the duration of the restriction. If you have digital records, you might want to move the data temporarily to a restricted drive or remove access to the file for the duration of the restriction.

There is more information on the ICO's website.

Please note our disclaimer: https://www.careprovideralliance.org.uk/disclaimer.html

The right to data portability

The right to data portability means that individuals have the right to be given the personal data which they have given to you in a "structured, commonly used and machine-readable format". They can only ask for this if your legal basis for processing this information is consent or for the performance of a contract *and* you hold the information digitally.

It is unlikely that this will happen often in social care and so there is not extensive guidance in this document. There is more information on the ICO's website.

The right to object

In certain instances, people can object to you processing their data. They can object to their data being used for direct marketing at any time and you must stop immediately – there are no exceptions to this.

They can also object if you are relying on public task or legitimate interests as your legal basis for processing. The individual must give you *specific* reasons why they object. You can decide to continue processing if you can demonstrate that you have compelling legitimate grounds for processing which override the interests, rights and freedoms of the individual or if the processing is necessary for a legal claim.

There is more information on the ICO's website.

Rights in relation to automated decision making and profiling.

It is very unlikely that you will be carrying out automated decision making or profiling in the course of your organisation's work. Automated decision making is when an assessment is made about an individual automatically through electronic methods, without any human input into that assessment. An example would be an online credit check to award a loan.

If you think this might apply to your organisation, there are specific rules which are now in force around automated decision making.

There is more information on the ICO's website.

Help!

If you are ever unsure on what you should do, then you should contact the ICO as they can provide help and guidance. Otherwise, you can contact the CPA for help on ig.feedback@careprovideralliance.org.uk.