Guidance on Data Protection: Community Hearing Care

This is a living document which the NCHA will update in response to new guidance from the Information Commissioner's Office (ICO).

We also welcome any feedback on how to improve this document and in particular how we can support micro to medium sized providers in the hearing sector meet new data protection requirements.

If you would like to be informed about updates to this guidance, or if you are a NCHA member and need additional support, please contact the NCHA.

ABOUT THIS UPDATED GUIDANCE

We published our initial data protection guidance in December 2017 to help community providers comply with the EU General Data Protection Regulation (GDPR) by the time it became law on 25 May 2018.

This updated guidance takes account of changes since December 2017, specifically:

- updated advice from the Information Commissioner's Office (ICO) and
- new UK Data Protection Act 2018 (DPA 2018) becoming law in May.

This update includes:

- simplified section on data protection regulations – possible because the DPA 2018 is now law
- additional detail on lawful bases for processing data – based on updated ICO guidance
- updated layout and headings – to aid dissemination.

The ICO still plans to issue new guidance in response to the DPA 2018. We will review new ICO advice and assess whether we need to update this guidance on a regular basis.

Contact us

Keep up to date with changes to this guidance and related sector news by contacting the NCHA, info@the-ncha.com.

NCHA members can contact us directly if they need any additional or bespoke advice. Please email info@the-ncha.com or call 020 7298 5110.

TABLE OF CONTENTS

INTRODUCTION

This guidance has been written by the National Community Hearing Association (NCHA) to help community-based hearing providers comply with data protection rules. It focuses on supporting micro to medium sized providers who might not always have the resources available to translate new rules into local effective polices. Larger providers can contact the NCHA directly for additional advice.

This guidance is in two parts:

- **Part one:** data protection at a glance – key points on the law, terms and responsibilities.
- **Part two:** what you need to do.

PART ONE: DATA PROTECTION AT A GLANCE

- **Part one will help you understand the new law, your overarching responsibilities and important key terms.** This will make it easier to complete part two of this guidance.

The good news is that many data protection concepts and principles have not changed – e.g. professional standards already require you to protect personal data. This means your existing polices will help you comply with the new law.

THE LAW

The General Data Protection Regulations (GDPR) came into force on 25 May 2018 across the EU. The GDPR allowed the UK to define certain 'terms and conditions' locally – e.g. including the definition of a health professional. The UK has done this using the Data Protection Act 2018 (DPA 2018). **The GDPR and DPA 2018 therefore have to be read together**. Throughout this guidance we use the term 'data protection law' to refer to the GDPR and DPA 2018.

KEY TERMS

Understanding the key terms in **Table 1** will make it easier to comply with new data protection rules.

Key terms	What it means
Principles (responsibilities)	**Data protection law sets out key principles for processing personal data.** Everything that follows in the law is informed by these principles. It is therefore important to understand and follow the spirit of the principles[1].

[1] ICO, Guide to the GDPR. Version 4 June 2018, p.15 accessed 27 June 2018

Personal data	**Data protection law only applies to personal data.** It applies to data held in electronic and paper form – i.e. not just paper records. Personal data is any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[2]
Non-personal data	**Data protection law does <u>not</u> apply to non-personal data** – e.g. it does not cover information you hold that is not about a natural person or anonymised data from which an individual cannot be identified[3]. **Information about companies or public authorities is <u>not</u> personal data**[4]. These data are therefore not subject to data protection law. The ICO states "**information about individuals acting as sole traders, employees, partners and company directors** where they are individually identifiable and the information relates to them as an individual **<u>may</u> constitute personal data**" [5] (our emphasis). Although data protection law does not apply to all the data you hold, data protection by design requirements mean that you are likely to benefit by taking steps to protect all your data.
Special categories of personal data	**Special categories of personal data require additional safeguards and an additional lawful basis for processing.** Special categories of personal data include data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, **data concerning health** or data concerning a natural person's sex life or sexual orientation.
Data controller	**The person(s) or organisation that determines the purposes and means of processing personal data** – usually the practice owner or company registered with the Information Commissioner.
Data processor	**The person(s) or organisation(s) responsible for processing personal data on behalf of the data controller** (other than a person who is an employee of the controller) – for example an external provider that manages payroll.
Data protection law	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) **<u>and</u>** Data

[2] Article 4(1), Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016

[3] Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016.
Note: Pseudonymised data might still fall within the scope of data protection law depending on how difficult it is to attribute the pseudonym to a particular individual (Ref: ICO, 21 Nov. 2017, Guide to the General Data Protection Regulations (GDPR))

[4] ICO, Guide to the GDPR. Version 4 June 2018, p.12 accessed 27 June 2018

[5] ICO, Guide to the GDPR. Version 4 June 2018, p.12 accessed 27 June 2018

	Protection Act 2018. Both need to be read together when considering data protection policies in the UK.
Lawful basis for processing	**There must be at least one lawful basis in order to process personal data**. If you process a special category of personal data you will need an additional - i.e. at least two - lawful basis for processing that data. The lawful bases are clearly explained in law (see Annex B).
Health professional	Health professional is defined in the Data Protection Act 2018. Health and Care Professions Council (HCPC) registrants are classified as health professionals in the UK[6]. Other EU Member States might have different definition of a health professional, it is therefore important to exercise caution when reading non-UK sources to design your data protection policies.

Table 1: Key terms in the GDPR and DPA 2018 2018.

KEY RESPONSIBILITIES (PRINCIPLES)

Community hearing providers will typically be data controllers. New data protection law[7] requires all data controllers to demonstrate compliance and accountability with the key responsibilities (principles) in Table 2. Part two of this guidance aims to help community hearing providers answer yes to questions in **Table 2.**

Responsibility[8]	**Question[9]**	
1. Lawful, fair and transparent	Is personal data processed lawfully, fairly and transparently?	☐ Yes ☐No
2. Purpose of limitation	Is personal data collected for specific, explicit and legitimate purposes and not used in an incompatible way with those purposes?	☐ Yes ☐No
3. Data minimisation	Is personal data adequate, relevant and limited to what is necessary for the intended purposes?	☐ Yes ☐No
4. Accuracy	Is personal data accurate and, where necessary, kept up to date – e.g. errors are rectified without undue delay?	☐ Yes ☐No
5. Storage limitation	Is personal data kept in a form which permits identification for no longer than is necessary?	☐ Yes ☐No
6. Security	Is personal data kept secure using appropriate technical or organisational measures – e.g. protecting against accidental loss, destruction or damage?	☐ Yes ☐No

Table 2: Overarching responsibilities (principles) in data protection law.

Community providers might also use data processors – e.g. software suppliers or an external agency to manage payroll**. It is very important to ensure that as a data controller you have GDPR compliant contracts in place with all data processors** as this will help meet the key responsibilities above.

[6] Data Protection Act 2018, Section 204
[7] Article 5 (2), Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016
[8] The full principles can be found in Article 5(1), Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016
[9] Adapted from text in ICO, Guide to the GDPR. Version 4 June 2018, accessed 27 June 2018

COMMON MYTHS

Some of the most common myths about the new law in the hearing sector can be found on page 7 of our initial guidance here.

PART TWO: WHAT YOU NEED TO DO

- **This section sets out what you need to do in four steps**. You will find it easier to follow if you read part one of this guidance first.

STEP ONE: GET EVERYBODY INVOLVED

- 80% of data security incidents involve staff, it is therefore important that all staff understand the organisation's data protection policies and that they are appropriately trained for their role [10].

Decision makers and key people: help your organisation comply with data protection requirements.

Employers: ensure all employees are aware that data protection laws have changed and

- what the practice/company is doing or planning to do to comply with new rules
- their own responsibilities in respect of practice and company operating procedures; and
- training and continuing professional development (CPD) opportunities in data protection and GDPR.

Employees: understand and follow your organisation's data protection policies.

STEP TWO: COMPLIANCE AND ACCOUNTABILITY

- One of the main changes to data protection law is that you have to demonstrate compliance and accountability with six key responsibilities – e.g. the new law requires you to identify and record the lawful basis for the personal data you process[11].
- This means hearing practices should keep documentation to demonstrate compliance and accountability with the new rules.

[10] ICO, 2016, Training checklist for small and medium sized organisations, version 1.3. accessed 27 November 2017
[11] ICO, Guide to the GDPR. Version 4 June 2018 accessed 27 June 2018

Record keeping and registration

The Information Commissioner's Office (ICO) has helpfully clarified that:

- "You are expected to put into place comprehensive **but proportionate** governance measures"[12] (our emphasis).

This means that for most hearing practices there will be little difference between protecting the data covered by the previous and new law – e.g. the fundamental basis for keeping health records has not changed which means that, on a daily basis, practices and practitioners will continue as now when processing most data. There is however now a need to keep records of processing activities.

The ICO has also confirmed

- "If you are processing data for the purposes of health administration and provision of patient care, then you will be required to register with the ICO"[13]

This means that hearing practices should continue to register with the ICO.

Based on data protection rules and ICO guidance hearing practices should therefore:

1. Register and maintain registration with the ICO.

2. Maintain a record of processing activities and how you protect this personal data. **The record should include[14]:**

a) name and contact details of the entity/person responsible for protecting personal data

b) a list of all the categories of personal data you hold - e.g. patient records, staff records, customer details etc. The list should include all personal data held in both paper and electronic formats. Remember you only have to do this for personal data

c) the lawful basis you use to process the data in your list – changes in the law mean that it will be important to understand (and be able to explain) the lawful basis you use to process personal data.

d) where possible, include the time limits for erasure of the different categories of personal data

e) where possible, include a general description of your technical and security measures – e.g. how you ensure ongoing confidentiality, integrity, availability and resilience of systems and services; how you would restore personal data in a timely manner in the event of a physical or technical incident; whether and how you test, assess and evaluate the effectiveness of technical and organisational security measures.

See Annex A for an example of what such a record might look like.

[12] ICO, 21 Nov. 2017, Guide to the General Data Protection Regulations (GDPR)
[13] ICO briefing in Issue 72 of HCPC In Focus, accessed 7 Dec 2017
[14] Article 30 of the GDPR 2016, adapted for community hearing care.

Understanding the lawful basis for processing personal data

- To comply with data protection law, you must identify at least one lawful basis for each general category of personal data.
- When processing a special category of personal data, you must have at least two lawful bases – i.e. one for general processing and one for processing the special category of data[15].
- **Annex A** includes an example of what a typical community practice might do.
- **Annex B** includes a full list of lawful bases with additional detail and examples.

You must have at least one lawful basis for processing personal data and document it. You should include the lawful basis/bases you use in your privacy notice[16].

It is important to note that the rights of the data subject will vary based on the lawful basis you use for processing personal data. It is also important to get this right because it is difficult to swap the lawful basis at a later date without good reason[17].

The lawful basis/bases you opt for might vary based on your specific business model, however in the hearing sector we expect most practices will use the following lawful bases:

- **legitimate interest and for the provision of health care**[18] – e.g. keeping patient record cards
- **for legitimate interests**[19] – direct marketing to existing customers[20]
- **for the performance of a contract with the data subject**[21] – e.g. employee records.

Annex B list all the lawful bases you might use, but below we offer more advice on

- legitimate interest – because the ICO has updated its guidance on this particular topic
- consent – because there is a lot of confusion and misinformation about this lawful basis in the context of hearing care in the UK.

Using legitimate interest as a lawful basis

Although legitimate interests is the most flexible lawful basis for processing personal data you must still be able to justify using it. If you decide to use legitimate interests as your lawful basis then "you are taking on extra responsibility for considering and protecting people's rights and interests"[22].

This additional responsibility does not have to be a complicated or costly process. To help, the ICO has produced a legitimate interest assessment (LIA). The LIA is a free "light-touch risk assessment" which can

[15] ICO, Guide to the GDPR. Version 22 March 2018, p.10. This means selecting a lawful basis from Article 6 and Article 9 of the GDPR.
[16] ICO, Guide to the GDPR. Version 22 March 2018, p.10, accessed 16 May 2018
[17] ICO, Guide to the GDPR. Version 22 March 2018, p.12, accessed 16 May 2018
[18] Article 9(2)(g) the GDPR
[19] Article 6(1)(f) the GDPR
[20] Slaughter and May, 2016, Processing of personal data: consent and legitimate interests under the GDPR, accessed 24 November 2017;
[21] Article 6(1)(b) the GDPR; and ICO, Guide to the GDPR. Version 4 June 2018 p. 84, accessed 27 June 2018
[22] ICO, Guide to the GDPR. Version 4 June 2018, p. 81. accessed 27 June 2018

be tailored to your specific circumstances[23]. There are three tests involved in the LIA and these are set-out in **Table 3**.

Test	Things to consider
1. **Purpose test:** are you pursuing a legitimate interest? You should be able to answer yes to this question. If not consider a different lawful basis.	Legitimate interest can include: your own interests or the interests of third parties, and commercial interests etc. The GDPR includes examples such as "client or employee data, marketing, fraud prevention, intra-group transfers, or IT security as potential legitimate interests, but this is not an exhaustive list"[24]. The types of questions the ICO suggests you might ask: ▪ Why do you want to process the data – what are you trying to achieve? ▪ Who benefits from the processing? In what way? ▪ What would the impact be if you couldn't go ahead? ▪ Would your use of the data be unethical or unlawful in any way?
2. **Necessity test**: is the processing necessary for the purpose test above? You should be able to answer yes to this question. If not consider a different lawful basis.	This means you must use personal data in a targeted and proportionate way of achieving your purpose identified in test 1 above – i.e. you cannot answer yes to this question if you can achieve the same outcome using another reasonable/less intrusive process. The types of questions the ICO suggests you might ask: ▪ Does this processing actually help to further that interest? ▪ Is it a reasonable way to go about it? ▪ Is there another less intrusive way to achieve the same result?
3. **Balancing test**: do the individual's interest override the legitimate interest? You should be able to answer no to this test. If not consider a different lawful basis.	This is the final test. You need to balance the interest you identified above against the individual's interests. These interests do not have to always align but you must be able to justify your decision. If the individual interests outweigh your interest then you should not use this lawful basis. The types of questions the ICO suggests you might ask: ▪ What is the nature of your relationship with the individual? ▪ Is any of the data particularly sensitive or private? ▪ Would people expect you to use their data in this way? ▪ Are you happy to explain it to them? ▪ Are some people likely to object or find it intrusive? ▪ What is the possible impact on the individual? ▪ How big an impact might it have on them?

Table 3: LIA for community hearing care[25].

Using consent as a lawful basis

There are some important factors to consider before using consent as the lawful basis.

[23] ICO, Guide to the GDPR. Version 4 June accessed 27 June 2018

[24] ICO, Guide to the GDPR. Version 4 June 2018, pp. 83 adapted accessed 27 June 2018.

[25] ICO, Guide to the GDPR. Version 4 June 2018, pp. 81-86 adapted accessed 27 June 2018.

Hearing practices should **NOT** use consent as the lawful basis for processing health care records or staff records. This is because the conditions for consent are unlikely to be met[26].

Data protection law in the UK also identifies HCPC registrants as health care professionals, therefore Hearing Aid Dispensers can use "for the provision of health care" as a lawful basis. This might not be the case in other EU Member States, so you should exercise caution if using international advice/articles to determine your lawful basis.

Consent is therefore likely to have limited applications in community hearing care in the UK – e.g. it might be used as the lawful basis for marketing to new customers in specific circumstances but **should not** be used as the lawful basis for processing health care records.

In some cases, practices might use consent of the data subject as the lawful basis for processing personal data. In cases where you do use customer consent as the lawful basis for holding/processing personal data, it is important that your consent processes comply with data protection law. In order to comply, consent must be:

1. given by a clear affirmative act – e.g. ticking a box when visiting an internet website, and therefore silence, pre-ticked boxes or inactivity will not meet this test
2. freely given, specific, informed and unambiguous – the data subject agreeing by a written statement, including by electronic means, or an oral statement
3. easy to withdraw.

NCHA members with any specific questions about the lawful bases they use, or about consent, can contact the NCHA directly for support.

Data processors and contracts

Community hearing care providers might use data processors – e.g. software suppliers to manage health records or an external agency to manage payroll. If you use data processors you need to **check your contracts comply with data protection law.** This is important because:

- data controllers and processors are liable for their compliance with data protection law, **but**
- data controllers must check that contracts with data processors comply with data protection law.

> The ICO published a checklist for contracts and it is important this is followed so that data controllers and data processors understand their responsibilities and liabilities.

[26] This is based on draft guidance from the ICO, 2017, Draft Consent Guidance. Please also note that GDPR states, "Where processing is based on the data subject's consent, […] Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment", it is the NCHA's view therefore – like the ICO and our primary care colleagues– that hearing care providers should not use consent as the lawful basis for processing health and employee records.

Data Protection Officers and Data Impact Assessment

Some, **but not all,** data controllers and processors will have to

- appoint a Data Protection Officer (DPO) and/or
- perform a Data Protection Impact Assessment (DPIA).

There is a lot of misinformation about DPOs and DPIAs in the public domain. It is important to note that:

- The vast majority of community hearing practices, given their size and scale of processing activities, will not have to appoint a DPO nor perform a DPIA.
- Community hearing care providers can now complete an ICO DPO self-assessment tool here.
- We recommend that members contact the NCHA before appointing a DPO.

You should consider the following points carefully before appointing a DPO or giving the title of DPO to a member of staff:

- the definition and scope of a DPO is very different under the new law. The DPO must have specialist knowledge of data protection law and work under conditions and terms specified in the new law
- therefore, hearing practices are advised **not** to give the DPO title to a member of staff simply because they lead on data protection for the organisation
- if an existing staff member has the title of DPO, but your organisation is not required to have a DPO under the new law, then change their title – e.g. to a Data Protection Lead or Data Protection Manager.[27]

STEP THREE: UNDERSTAND INDIVIDUAL RIGHTS

Changes to data protection law strengthen individual rights when it comes to their own personal data. Individuals have eight rights. This section focusses on two of these rights, the right to be informed and the right to access – see **Annex C** for a full list.

Right to be informed: privacy notice

A privacy notice explains how you process data, and the procedures you use to deal with data queries and problems. Ensure your privacy notice is kept up to date and any significant changes are communicated to all affected data subjects[28].

[27] Article 29 Working Party, 2017, Guidelines on Data Protection Officers, ec.europa.eu/newsroom/document.cfm?doc_id=44100 accessed 27 November 2017

[28] The privacy statement is a required as part of an individual's right to be informed, Article 13 and 14 of the GDPR.

You will find it easier to write your privacy notice if you complete the sections above first. For example, you will need the information you gather from doing step one and two above in order to write your privacy notice.

Your privacy notice should be

- concise and transparent
- easy to understand and access; and
- free of charge.

What the privacy notice contains will depend on how you obtain and process personal data, but briefly it should include:

- the data controller details;
- what personal data you process and why, and where possible how long you keep it for
- the purpose of processing this data, and the lawful basis
- whether you share it with any other party, and if so why
- an explanation of how to withdraw consent or opt-out of marketing - e.g. if you have used consent as lawful basis for processing then make clear the individual can withdraw consent at any time, if you have used legitimate interests for marketing the individual can also opt-out of marketing
- how to lodge a complaint with the ICO.

For further details on what to include in a privacy statement, see ICO advice here.

Right to access: responding to requests

A Subject Access Request (SAR) allows individuals to access personal data that is held about them in any format (subject to some safeguards). Under new rules:

- you must respond to a SAR within **one month** you can no longer charge a person making a SAR, unless a request is manifestly unfounded or excessive – e.g. for multiple further copies of the same information[29]
- if you can charge for a SAR then this must not be more than the administrative cost of providing the information[30] - e.g. if you have provided a copy of a prescription following a hearing test and a customer asks for a second copy then you will be able to charge a fee for the copy that is no more than the administrative cost of providing the information.

[29] ICO, 2017, Overview of the General Data Protection Regulation (GDPR) page 30, accessed 15 September 2017
[30] ICO, 2017, Overview of the General Data Protection Regulation (GDPR) page 30, accessed 15 September 2017

STEP FOUR: ENSURE PROCESSES HELP YOU MEET ONGOING REQUIREMENTS

Complying with data protection law is an ongoing process, this means you will need to have systems in place to ensure you are always meeting your obligations to protect personal data. This is particularly important when processing special categories of personal data – e.g. health records.

Data protection by design

> You should now "meet the principles of data protection by design and data protection by default"[31]. This means you need to consider data protection and privacy issues in everything you do.

Data protection law requires you to "put into place comprehensive **but proportionate** governance measures"[32] (our emphasis). This means small companies will not be expected to invest large sums in state of the art defence systems, but instead they will be expected to "put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights"[33].

Data protection law only applies to personal data – i.e. not any other information you hold. However, if for example you use a computer system to store both personal and non-personal data, applying data protection by design principles across your business will help you comply with data protection law.

Implementing the Government backed Cyber Essentials scheme is a good starting point for complying with data protection law[34]. This is a free tool that allows you to self-certify using five technical controls that you should implement:

1. use a firewall to ensure you have secure internet connection
2. choose the most secure settings for all devices and software – e.g. using robust passwords
3. control who has access to data and services – e.g. setting permissions based on staff responsibilities
4. protect against viruses and malware – e.g. using anti-virus/malware software at all times
5. keep devices and software up to date – e.g. set devices to automatic update and understand which devices/software are no longer supported and take appropriate action.

You can access a free Cyber Essentials checklist at bottom of this webpage. The following resources might also be helpful:

- ICO practical guide to IT security for small business here[35]
- National Cyber Security Centre infographic for small business.

[31] ICO, 21 Nov. 2017, Guide to the General Data Protection Regulations (GDPR)
[32] ICO, 2017, Overview of the General Data Protection Regulation (GDPR) page 30, accessed 15 September 2017
[33] ICO, Guide to the GDPR. Version 4 June 2018, p. 174 accessed 27 June 2018
[34] National Cyber Security Centre, About, Cyber Essentials and GDPR, accessed 10 July 2018
[35] ICO, 2016, A practical guide to IT security, Ideal for the small business

Demonstrating that reasonable steps have been taken to protect personal data will reduce the risk of reputational damage and financial sanctions that may result from any potential data breach.

Reporting a data breach to the ICO

A personal data breach is any breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. You do not have to report all breaches but should learn from every event – e.g. near misses – in order to reduce future risks.
You have to report a data breach where it is likely to result in a risk to the rights and freedoms of individuals, which if left unaddressed could cause a 'significant detrimental effect'. This includes breaches resulting in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

In the event of a serious breach the ICO must be notified within **72 hours without undue delay.**

A breach report should include the following information:
- nature of the breach
- numbers of individuals affected
- actions being undertaken to rectify the breach; and
- data controller's or reporter's name and contact details

Details of how to notify the ICO of a breach can be found here.

Informing individuals affected

Individuals affected must also be notified if the breach is likely to result in a 'high risk' to their individual freedoms. More details can be found on the ICO website.

Data controllers/processors will need to look at the facts of a breach and decide on a case by case basis what needs reporting.[36]

The NCHA will be able to advise members in individual cases, although you should seek help as soon as possible to ensure you can report necessary breaches to the ICO within the required time frame.

OTHER USEFUL INFORMATION

Health care records

The ICO has confirmed that "patient consent for treatment or to share health care records is **not the same** as GDPR consent" and that in a UK health care setting "consent is often **not the appropriate lawful basis under the GPDR**"[37] (our emphasis).

[36] ICO, 21 Nov. 2017, Guide to the General Data Protection Regulations (GDPR)
[37] ICO, GDPR FAQs for small health sector bodies, https://ico.org.uk/for-organisations/health/health-gdpr-faqs/, accessed 11 July 2018.

Data protection law complements, rather than replaces, existing best practice guidance and standards on record keeping in health care. Hearing care professionals should continue to follow:

- HCPC standards, e.g. Confidentially – guidance for registrants[38], Standards of proficiency – Hearing aid dispensers[39]
- sector specific guidance on record keeping – e.g. BSHAA guidance on professional practice Hearing Aid Audiologists[40]

UK data protection law classifies health records as a special category of data "for health care purposes" and acknowledges that HCPC registrants are health care professionals. Annex A provides an example of the lawful bases providers using HCPC registrants might use for processing health information.

Staff Records and Personnel Data

As noted above, staff records cannot be held merely on the basis of employee consent. There are several reasons for this, including because of the imbalance of power between employer and employee precludes genuine free choice. So there is no need to ask staff to sign consent forms for their data to be held for personnel purposes. It is however, as with all personal data you process, important to only process personal data in accordance with key principles and always respect the data subject's rights.

Staff records and personnel data are normally processed on one of the following legal bases:
- for performance of the employment contract
- in order to comply with legal obligations - e.g. on tax and pensions
- legitimate interests of the practice/business.

Customer data for other purposes – e.g. advertising and marketing etc.

New data protection rules do not cover all circumstances in which personal data is collected or used. For the purposes of marketing, in the context of this guidance, businesses should also ensure customer data is processed in a way that complies with
- new data protection requirements
- the Privacy and Electronic Communications Regulations (PECR)[41].

Businesses might find the following ICO resources helpful
- Direct Marketing, PECR – long form
- Direct Marketing – checklist
- Cyber Essentials scheme

[38] HCPC, 2017, Confidentially – guidance for registrants
[39] HCPC, 2014, Standards of proficiency – Hearing aid dispensers
[40] BSHAA, Guidance on professional practice Hearing Aid Audiologists
[41] PECR also originates from an EU Directive and is in the process of being updated. We will update guidance once the new regulations are published, subject to how EU regulations are implemented in the UK after March 2019

WHAT NEXT?

We welcome any feedback on how to improve this document and in particular how we can support micro to medium sized providers in the hearing sector meet new data protection requirements.

The ICO plans to issue new guidance in response to the DPA 2018. We will review new ICO advice and assess whether we need to update this guidance on a regular basis.

Keep up to date with changes to this guidance and related sector news by contacting the NCHA, info@the-ncha.com.

NCHA members can contact us directly if they need any additional or bespoke advice. Please email info@the-ncha.com or call 020 7298 5110.

National Community Hearing Association
July 2018

ANNEX A - EXAMPLE OF RECORD KEEPING IN TYPICAL COMMUNITY HEARING PRACTICE

Name of Controller: Click here to enter text.
Address of Controller: Click here to enter text.
Telephone/Email: Click here to enter text.
Responsible person: Click here to enter text.

Category of personal data/data subject	Legal basis for processing personal data	Who these personal data are shared with	Where possible, time limits for erasure	Technical/organisational security measures to ensure level of security appropriate to risks
Patient records – including test results, imaging, referral letters etc.	Legitimate interest **and** for the purposes of health care	Registered health care professionals and those under their supervision	See footnote 42 Adults: 8 years[43]. Children: retained until aged 25 (or 26 if they are 17 when treatment ends)[44]	Registered health professionals and those under their supervision have access. All registered staff comply with HCPC standards, which ensure they respect patient confidentiality and make accurate records. Paper records are kept securely. Electronic data is password protected and employees can only access the information essential for their role, and receive appropriate training for their role. All employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date.
Customer records – e.g. direct debit/payment details	Legitimate interest	The data subject's bank	Kept for tax purposes and future claims/information	Paper records are kept securely. Electronic data is password protected and employees can only access the information essential for their role, and receive appropriate training for their role. All employees have passwords so there is an audit of any changes made, there is also a back-up system that means data can be restored. All anti-virus software and other software are kept up to date.
Staff records – includes bank details, NI number, and other personal information	Performance of a contract with the data subject or to take steps to enter into a contract and processing is necessary for carrying out obligations under employment	HR (including payroll) and senior management only	Kept for tax purposes and future claims/information	

Table A1: Example of how a community hearing practice might document its compliance with data protection rules.

[42] Retention periods, listed above, reflect minimum requirements. Health records may be required as evidence in legal actions and then be kept as advice by legal representatives.
[43] In the absence of sector specific guidance, this is based on BMA guidance of 8 years for other hospital records accessed 7 December 2017 https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/retention-of-health-records
[44] NHS, How long should medical records (health records) be kept for? https://www.nhs.uk/chq/Pages/1889.aspx?CategoryID=68 accessed 7 December 2017. More information can be accessed at NHS Digital - https://digital.nhs.uk/data-security-information-governance

ANNEX B – LAWFUL BASES FOR PROCESSING PERSONAL DATA

- Practices will need to have **at least one** lawful basis from **Table B1** for each processing activity.
- **In addition** practices will need to select a lawful basis from **Table B2** when processing a special category of personal data – e.g. health care records. Your choice of lawful basis from **Table B1** does not dictate your choice of lawful basis from **Table B2** vice versa – e.g. if you use consent as your lawful basis in table B1 you do not have to use consent from Table B2[45].
- Special categories of personal data include data: revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, **data concerning health** or data concerning a natural person's sex life or sexual orientation.
- Please note that the ICO intends to issue more detailed guidance on the new special category conditions in the Data Protection Act 2018 in due course[46]. The NCHA will review that guidance any update **Table B2** accordingly.
- You can also complete the ICO's interactive toolkit if you are unsure which lawful basis to use and/or contact the NCHA for support.

[45] ICO, Guide to the GDPR. Version 4 June 2018, p.88 accessed 27 June 2018
[46] ICO, Guide to the GDPR. Version 4 June 2018, p.87 accessed 27 June 2018

Table B1: Lawful basis for general processing.

Basis for processing personal data (ICO)[47]	Legal wording in the GDPR	Notes/examples for community hearing care providers in the UK[48]
Consent: the individual has given clear consent for you to process their personal data for a specific purpose.	See Article 6(1)a here	Most likely to be the lawful basis when data is processed for marketing to new customers. Should **NOT** be used as the lawful basis for health records or employee records.
Contract: processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract	See Article 6(1)b here	Might be used, for example employment contract. But note it does not apply if you need to process one person's details but the contract is with somebody else[49].
Legal obligation: processing is necessary for you to comply with the law (not including a contractual obligation)	See Article 6(1)c here	Might be used, for example to comply with tax law. Note this legal obligation has to have "a sufficiently clear basis in either common law or statute", it is not necessary to cite each specific piece of legislation[50]
Vital interests: processing is necessary to protect someone's life	See Article 6(1)d here	Not applicable for community hearing care providers. For example, the ICO notes that this is less likely to be appropriate for care that is planned in advance[51].
Public task: processing is necessary for you to perform a task in the public interest or for your official functions, and the task has a clear basis in law	See Article 6(1)e here	Unlikely to be the most suitable lawful basis for community hearing care providers.
Legitimate interest: processing is necessary for your legitimate interests or legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (A public authority cannot use this lawful basis to perform an official task)	See Article 6(1)f here	Likely to be the lawful basis for most personal data held by practices (note that health records will also require you to pick a lawful basis from table B2 – see Annex A for an example) You should check this is the most appropriate lawful basis by completing a legitimate interest assessment (LIA).

[47] ICO, Guide to the GDPR. Version 4 June 2018, p.53-54 accessed 27 June 2018
[48] Please note, outside the UK different lawful bases and definitions of health care professional might apply
[49] ICO, Guide to the GDPR. Version 22 March 2018, p.30 accessed 16 May 2018
[50] ICO, Guide to the GDPR. Version 22 March 2018, p.30 accessed 16 May 2018
[51] ICO, Guide to the GDPR. Version 22 March 2018, p.34 accessed 16 May 2018

Table B2: lawful basis for processing a special category of data. Green boxes show those most likely to be used in community practice.

Basis for processing special categories personal data (ICO)	Full legal wording	Notes/examples for community hearing care providers in the UK[52]
Data subject has given explicit consent to process a special category of data and it is not prohibited by the UK Data Protection Act 2018	See Article 9(2)a here and DPA 2018	UK community hearing practices are very unlikely to rely on this lawful basis. The Data Protection Act 2018 defines HCPC registrants as health professionals, and community hearing care providers can use Article 9(2)(h) instead, highlighted in green below.
Necessary **for the purposes employment, social security and social protection**	See Article 9(2)b here and DPA 2018	Might be used by community hearing practices.
Necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent	See Article 9(2)c here and DPA 2018	Unlikely to apply in community hearing care.
Carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim	See Article 9(2)d here and DPA 2018	Unlikely to apply in community hearing care.
Relates to personal data which are manifestly made public by the data subject	See Article 9(2)e here and DPA 2018	Unlikely to be used by community hearing practices.
Necessary for the **establishment, exercise or defence of legal claims**	See Article 9(2)f here and DPA 2018	Might be used by community hearing practices.
Necessary for reasons of substantial public interest	See Article 9(2)g here and DPA 2018	Unlikely to be used by community hearing practices.
Necessary for the […] the provision of health or social care or treatment or the management of health or social care systems and services	See Article 9(2)h here and DPA 2018	Will be used by most community hearing practices for processing health care records. This provision is available to health care professionals as recognised in UK law – e.g. HCPC registrants.
Necessary for reasons of public interest in the area of public health	See Article 9(2)I here and DPA 2018	Unlikely to be used by community hearing practices.

[52] Please note, outside the UK different lawful bases and definitions of health care professional might apply

Necessary for archiving purposes in the public interest, research and statistics where allowed by UK law	See Article 9(2)j here and DPA 2018	Unlikely to be used by community hearing practices.

ANNEX C - INDIVIDUAL RIGHTS

Table C sets out the eight rights individuals have under data protection law. Some of these rights might not apply in certain circumstances.

Right	What does this mean in my hearing practice?
The right to be informed	▪ Be transparent about how you use personal data by letting customers have access to 'fair processing information' – e.g. sharing an up to date and accurate privacy notice. ▪ Ensure your privacy notice is: concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.
The right of access	▪ If you process personal data then individuals – e.g. customers, patients, staff – can ask for copies of their own personal data. ▪ This is often referred to as a Subject Access Request (SAR). ▪ The Data Protection Act 2018 makes it an offence to make any amendment with the intention of preventing its disclosure.
The right to rectification	▪ Individuals can ask you to rectify personal data if it is inaccurate or incomplete. ▪ Respond to such requests within one month, although if it is a complicated request you might be able to extend this by two months.
The right to erasure	▪ This is also known as 'the right to be forgotten' – e.g. a person might be able to ask you to delete or remove personal data you hold on them. ▪ This applies where there is no compelling reason for its continued processing. It is **not** applicable where there is a duty to keep accurate health records and you have selected the correct lawful basis for keeping health records in the UK[53].
The right to restrict processing	▪ A customer has the right to 'block' or suppress you processing their data in certain circumstances. This is unlikely to apply in a typical hearing practice. If there is a basis for a customer to exercise this right then you can store the personal data, but not further process it.
The right to data portability	▪ This is unlikely to apply to community hearing practice because it applies when processing is carried out by automated means.
The right to object	▪ Individuals can object to you processing their personal data in certain circumstances. ▪ If you used "legitimate interest" as the lawful basis for processing personal data and an individual objects you must stop processing data **unless** you can a) demonstrate how your legitimate interests override the interests, rights and freedoms of the individual or b) you are processing the data for the establishment, exercise or defence of legal claims. ▪ If an individual objects to you processing personal data for direct marketing, you must stop processing data for that purpose.

[53] ICO, Guide to the GDPR. Version 4 June 2018, p.120, accessed 11 July 2018

The right not to be subject to automated decision-making including profiling	▪ This is unlikely to apply in community hearing care settings.

Table C: Individual rights under new data protection law, ICO, 22 March 2018, Guide to the General Data Protection Regulations (GDPR) pp. 51-112 adapted for community hearing care