

NHS Grampian

Information Governance – Data Protection

NHS Grampian Privacy Notice

Revision history

Date	Activity	Authority
21 December 2022	Revised NHS Scotland privacy notice template released for use.	Short Life Working Group of NHS Scotland IG Leads Forum.
5-10 January 2023	Localised for NHS Grampian with additional sections added, including comment from professional peers.	Head of Information Governance and DPO, NHS Grampian.
5-10 January 2023	Draft shared with NHS IG Leads/DPOs in North of Scotland region for informal peer-review.	IG Leads/DPOs of NHS Highland, Orkney, Shetland, Tayside and Western Isles.
6 January 2023	Draft shared with DPOs from Aberdeen City Council, Aberdeenshire Council and Moray Council re partnership working.	DPOs of Aberdeen City, Aberdeenshire and Moray Councils.
11 January 2023	Considered and approved for publication.	Information Governance Steering Group, NHS Grampian.
17 June 2026	Periodic review and approved for publication	Medical Director, Caldicott Guardian and SIRO

CONTENTS

1. About NHS Grampian and our key relationships	p3
2. About the personal information we use	p3
3. Our purposes for using personal information	p4
4. Our legal basis for using personal information	p5
5. Who provides the personal information	p6
6. Sharing personal information with others	p6
7. Transferring personal information abroad	p11
8. Retention periods of the information we hold	p11
9. How we protect personal information	p11
10. Your rights (including how to request your personal data and how to contact our Data Protection Officer)	p11

1. About NHS Grampian and our key relationships

Grampian Health Board, commonly known as NHS Grampian, is a public organisation (a Scottish Health Board) created in Scotland under section 2 of the National Health Service (Scotland) Act 1978 (the **1978 Act**). It is one of the organisations which form part of NHS Scotland (**NHSS**).

As NHS Grampian is just one part of the integrated health and social care system in Scotland, you should read this privacy notice in conjunction with those provided by your GP or other primary care provider (such as your NHS dentist, optometrist or pharmacist) and the information provided nationally on the [NHS Inform](#) website, the [Public Health Scotland](#) website, the [NHS National Services Scotland](#) website, and the website of [NHS Education for Scotland](#). NHS National Services Scotland and NHS Education for Scotland are being merged as NHS Public Services Delivery Scotland during 2026 and new privacy information is likely to follow on the new website. Members of the public are encouraged to search for any new privacy information published by the new organisation in due course.

We work in close partnership with our colleagues in [Aberdeen City Council](#), [Aberdeenshire Council](#), and [Moray Council](#) around the delivery of health and social care, further to the provisions of the Public Bodies (Joint Working) (Scotland) Act 2014 and under the delegated authority of the three Integration Joint Boards in the region: [Aberdeen City](#); [Aberdeenshire](#); and [Moray](#). Please note that integrated services are delivered under the banner of the relevant 'Health and Social Care Partnership'.

Our headquarters are: NHS Grampian, Summerfield House, Eday Road, Aberdeen.

Our main switchboard number is: 0345 456 6000.

Our Information Commissioner's Office registration number is Z8547986.

2. About the personal information we use

We use personal information on different groups of individuals including:

- Patients and their legal representatives, guardians or close family members or associates such as their Next of Kin;
- Staff, volunteers, students and applicants;
- Contractors;
- Suppliers;
- Complainants, enquirers;
- Survey respondents or research participants;
- Professional experts and consultants;
- Individuals captured by CCTV.

The personal information we use (personal data) includes information that identifies you like your name, address, date of birth, postcode or Community Health Index (CHI) number. Your CHI number is a unique identifier used across the healthcare system in Scotland.

We also use more sensitive types of personal information (special categories of personal data), including information about racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic and biometric data, health; sex life or sexual orientation.

The information we use can relate to personal and family details; education, training and employment details; financial details; lifestyle and social circumstances; goods and services; visual images; details held in the patient record; responses to surveys etc.

3. Our purposes for using personal information

Under the 1978 Act NHS Grampian has a statutory responsibility to provide or arrange for the provision of a range of healthcare, health improvement and health protection services. We are given these tasks so that we can help to promote the improvement of the physical and mental health of the people of Grampian and assist in operating a comprehensive and integrated national health service in Scotland.

We use personal information to enable us to: provide healthcare services for patients (including reminding you of appointments); to undertake data matching under the

national fraud initiative and for fraud prevention; when supporting and managing our employees; to maintain our accounts and records; in partnership with local authorities for the purposes of health and social care management and delivery; to facilitate fundamental medical research; for the analysis needed to manage the health and social care system; to share data into appropriate health care registries such as those maintained by Public Health Scotland; and for the prevention and detection of crime, including the use of CCTV systems.

For more information on the activities that use personal data in a Scottish Health Board and why that is likely to be lawful, please see the table published online at <https://www.nhsgrampian.org/about-us/data-protection/>.

4. Our legal basis for using personal information

NHS Grampian, as data controller, is required to have a legal basis when using personal information. NHS Grampian normally considers that performance of our tasks and functions are in the public interest and further to our official authority under the 1978 Act. So, when using personal information our legal basis is usually that its use is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in us. In some situations, we may rely on a different legal basis; for example, when we disclose personal information to comply with a legal request (e.g. a court order), our legal basis is that its use is necessary to comply with the legal obligation. Another example would be for compliance with a legal obligation to which NHS Grampian is subject. For example, we have a duty under the Public Health etc (Scotland) Act 2008 to notify Health Protection Scotland when someone contracts a specific disease.

When we are using more sensitive types of personal information (special categories of personal data), including health information, our legal basis is usually that the use is necessary:

- for the provision of health or social care or treatment or the management of health or social care systems and services; or
- for reasons of public interest in the area of public health; or

- for reasons of substantial public interest for aims that are proportionate and respect people's rights; or
- for archiving purposes, scientific or historical research purposes or statistical purposes, subject to appropriate safeguards; or
- in order to protect the vital interests of an individual; or
- for the establishment, exercise, or defence of legal claims or in the case of a court order.

On rare occasions we may rely on your explicit consent as our legal basis for using your personal information. When we do this, we will explain what it means, and the rights that are available, to you.

Please Note: we may also ask for your consent for us to perform specific healthcare procedures or operations, or when you take part in drug trial. This is known as **clinical** or **ethical** consent. It demonstrates that you have agreed to receive a particular type of care or to participate in an activity. In these circumstances we will not normally be relying on your **clinical** consent as the lawful basis for our processing of your personal data. Where you have provided consent for the processing of your personal information, we will make it clear to you that you have the right to withdraw that data processing consent at any point.

For more information on the activities that use personal data in a Scottish Health Board and why that is likely to be lawful, please see the table published online at <https://www.nhsgrampian.org/about-us/data-protection/>.

5. Who provides the personal information

When you do not provide information directly to us, we receive it from other individuals and organisations involved in the delivery of health and social care services in Scotland. These include other NHS Boards and primary care contractors such as GPs, dentists, pharmacists and opticians, other public bodies e.g. Local Authorities and suppliers of goods and services.

6. Sharing personal information with others

Depending on the situation, where necessary we will share appropriate, relevant and proportionate personal information in compliance with the law, with the following:

- Our patients and their chosen representatives or carers;
- Staff;
- Current, past and potential employers;
- Healthcare social and welfare organisations;
- Suppliers, service providers, legal representatives;
- Auditors and audit bodies;
- Educators and examining bodies;
- Research organisations;
- People making an enquiry or complaint;
- Financial organisations;
- Professional bodies;
- Trades Unions;
- Business associates;
- Police forces;
- Security organisations;
- Central and local government;
- Voluntary and charitable organisations.

Where the Board shares information with other organisations it will normally do so further to the provisions of an Information Sharing Agreement. Where the Board appoints another organisation or supplier to act on its behalf, that organisation or supplier will be subject to the provisions of a data processing agreement.

Please note that the agreements for many of the systems and services used by NHS Grampian are negotiated by national Boards, such as NHS National Services Scotland or NHS National Education Scotland, on behalf of all Scottish Health Boards.

Where information requires to be shared in extremis, for example for the preservation of life or in a major emergency, NHS Grampian will do so. You may wish to review the guidance from the Information Commissioner around [Data sharing in an urgent situation or in an emergency](#).

There are some common situations where data is shared routinely and we wanted to make you aware of those. We share data:

6a. with other parts of NHS Scotland

Within the NHS in Scotland, data is shared between Health Boards and organisations including the Scottish Ambulance Service, Public Health Scotland (PHS), NHS 24, and between Health Boards, GPs, community optometrists, community dentists and pharmacists for the purposes of your health or social care, the management of the health and social care system and when responding to public health issues. The Intra NHS Scotland Information Sharing Accord and the Joint Data Controller and Information Sharing Agreement between Health Boards and GP practices are examples of agreements used for this sort of data sharing.

Sharing across the NHS in Scotland includes working at national and regional level as well as in direct partnership with other Boards or NHS organisations. NHS Grampian is part of the East of Scotland sub-national planning arrangements for the NHS and works collaboratively with other Health Boards across Scotland.

6b. with local authorities

We work with our local authority partners for the purposes of health and social care integration further to the integrated approach to health and social care under the Public Bodies (Joint Working) (Scotland) Act 2014. We have signed an Information Sharing Protocol for integrated functions with each of the three local authorities in Grampian. This involves working very closely as partners and means that appropriate health information is shared with local authorities and appropriate social care information is shared by local authorities with the NHS Grampian for the purposes of your care. The goal is to facilitate an integrated, multi-disciplinary, model for health and social care, centred on you.

We also collaborate on joint planning of the health and social care system in areas such as improving discharge planning or understanding service capacity pressures. This involves the use of anonymous statistical data about our patients and their healthcare conditions and needs, or the state of the health and social care system.

6c. with other agencies

There are key statutory purposes for which we share data routinely between relevant partners and agencies such as Police Scotland, Scottish Fire and Rescue, local authorities and relevant Scottish and UK government agencies. They include child or adult public protection matters, emergency planning and response (including planning for and responding to major incidents), the prevention and detection of crime and responding to public or environmental health issues.

Statistical data, which may be drawn from an analysis of your health data but is unlikely to identify you, is shared with Scottish and UK Governments for the purposes of statutory reporting and national planning.

We share information with national agencies such as the Driver and Vehicle Licensing Agency, the Medicines and Healthcare products Regulatory Agency, or NHS England as part of UK wide initiatives where it is relevant for your health or social care, public safety or for important purposes of public health or medicines or device safety.

6d. with regulators

If a professional or conduct matter is raised by one of the relevant professional registration bodies, that can lead to the professional body requesting access to your health records under their statutory powers. The focus of these requests is the professional person or matter being investigated rather than you, but your records may be essential to the regulator understanding the issue they are examining. In such cases, NHS Grampian will work with the applicable professional body to help make sure that any of your data passed to them is appropriate and will be managed securely.

We are audited regularly by external regulators who have a statutory duty to make sure that we are performing appropriately. That can include the regulator reviewing patient information and records to satisfy itself that appropriate standards are being met. Healthcare Improvement Scotland, the Care Inspectorate, Audit Scotland and

the Health and Safety Executive are all examples of regulators who oversee our work.

6e. with researchers

Approved medical research also takes place using healthcare data. Where this involves several healthcare providers it is normally considered via the Public Benefit and Privacy Panel and/or relevant ethics committees (such as university ethics committees when we work with clinical academic colleagues).

Approval for participation in national or local research is given by the NHS Grampian's Caldicott Guardian, who is a senior clinician. In NHS Grampian the Caldicott Guardian is the Medical Director, who also has two Deputy Caldicott Guardians supporting them.

Research can include the provision of data, including identifiable data, to national registries for long-term analysis of trends in particular conditions for the benefit of everyone.

Research in health care also comprises the aggregation (bringing together) of data from different parts of the health and social care system. The outputs of research are always anonymous, are not used to make decisions about and safeguards will be put in place to help ensure the use of your data will never be harmful to you.

NHS Grampian and the University of Aberdeen have partnered in setting up a Data Safe Haven (DaSH) to facilitate appropriate and approved health research. NHS Grampian and the University have an agreement governing the operation of DaSH, and it is overseen via a joint group comprising members of NHS Grampian and the University. DaSH operates under a series of Standard Operating Procedures and technical security controls to help ensure the security of the health data processed for approved research.

Where data is processed for medical research purposes, the lawful bases for doing so are normally that it comprises a task in the public interest and under the official authority of NHS Grampian and research purposes subject to the safeguards in Article 89(1) of UKGDPR.

7. Transferring personal information abroad

NHS Grampian does not transfer personal data outside of the UK routinely. When information is transferred outside the UK, the Board ensures that appropriate safeguards are in place per the terms of data protection legislation.

8. Retention periods of the information we hold

NHS Grampian, like all Scottish Health Boards, is subject to the Scottish Government's Records Management Code of Practice for Health and Social Care - <https://www.gov.scot/publications/records-management-code-practice-health-social-care/>. The Code of Practice sets out minimum retention periods for information, including personal information, held in different types of records including personal health records and administrative records. NHS Grampian aligns its activity with that Code of Practice.

9. How we protect personal information

We take care to ensure your personal information is only accessible to authorised people. Our staff have a legal and contractual duty to keep personal health information secure, and confidential. Our clinical staff are also subject to professional obligations via their registration body (General Medical Council; Nursing and Midwifery Council; Health and Care Professions Council; General Dental Council; General Pharmaceutical Council; General Optical Council etc). The following security measures are in place to protect personal information:

- All staff undertake mandatory training in Data Protection and IT Security;
- Information Security policies and procedures are in place and checked regularly against the requirements of relevant legislation;
- We have access controls for our systems and can audit activity.

10. Your rights

This section contains a description of your data protection rights within NHS Grampian.

10a. The right to be informed

NHS Grampian must explain how we use your personal information. We use a number of ways to communicate how personal information is used, including:

- This Data Protection Notice and additional privacy notices provided to you directly in respect of certain activities or processes;
- Information leaflets;
- Discussions with staff providing your care.

10b. The right of access

You have the right to access your own personal information.

This right includes making you aware of what information we hold along with the opportunity to satisfy you that we are using your information fairly and legally.

You have the right to obtain:

- Confirmation that your personal information is being held or used by us
- Access to your personal information
- Additional information about how we use your personal information

Although we must provide this information free of charge, if your request is considered unfounded or excessive, or if you request the same information more than once, we may charge a reasonable fee.

If you would like to access your personal information, you can do this by submitting a written request to the following address:

NHS Grampian, Information Governance Team, Rosehill House, Cornhill Road,
Aberdeen

E: gram.infogovernance@nhs.scot

T: 01224 551549

Please note, emails from your private email address may not be secure, so please consider carefully how much information you include. If you would like some guidance on sending information securely, please let us know.

Once we have received your request and you have provided us with enough information for us to locate your personal information, we will respond to your request without delay, within one month (30 days). However, if your request is complex, we may take longer, by up to two months, to respond. If this is the case, we will tell you and explain the reason for the delay.

We have a standard form that you can use to help you make your request online here - <https://www.nhsgrampian.org/about-us/confidentiality-health-records-and-data-protection/>.

You should note that if you are requesting your medical information, we will ask you to verify your identity. Given the significance of this data, you will understand that we must be certain that we are releasing information to the right people.

You can nominate a representative to make a request on your behalf, such as you solicitor. We have a form to help with that too, which is linked on the same page as the one you can use to help make a request directly (link above).

10c. The right to rectification

If the personal information we hold about you is inaccurate or incomplete you have the right to have this corrected.

If it is agreed that your personal information is inaccurate or incomplete, we will aim to amend your records accordingly, normally within one month, or within two months where the request is complex. However, we will contact you as quickly as possible to explain this further if the need to extend our timescales applies to your request. Unless there is a risk to patient safety, we can restrict access to your records to ensure that the inaccurate or incomplete information is not used until amended.

If for any reason we have shared your information with anyone else, perhaps during a referral to another service for example, we will notify them of the changes required so that we can ensure their records are accurate.

If, having considered your request, NHS Grampian does not agree that your data is inaccurate, we may add a comment to your record stating your concerns about the information. If this is case, we will contact you within one month to explain our reasons for this.

10c. The right to object

When NHS Grampian processes your personal information for the purpose of the performance of a task carried out in the public interest or in the exercise of official authority you have the right to object to the processing and also seek that further processing of your personal information is restricted. We are happy to consider any such requests, but please note that where NHS Grampian can demonstrate compelling legitimate grounds for processing your personal information, for example in respect of patient safety, clinical recordkeeping or in support of legal claims, it is unlikely that we will be able to restrict the processing of your data.

10d. Rights in relation to automated decision-making and profiling

NHS Grampian does not, at present, make any decision based solely on automated processing or profiling.

10e. Other rights

There are other rights under data protection legislation, however these rights only apply in certain circumstances, many of which are not applicable in respect of the processing data for the purposes of the provision of healthcare. For further information on these rights please see ico.org.uk/for-the-public. If you have any questions, please do let us know.

10f. The right to complain

We employ a Data Protection Officer to check that we handle personal information in a way that meets data protection law. If you are unhappy with the way in which we use your personal information or any decision we have made in respect of your data rights, please tell our Data Protection Officer using the contact details below.

Data Protection Officer, NHS Grampian, Information Governance Team, Foresterhill Lea, Foresterhill Rd, Foresterhill Health Campus, Aberdeen, AB25 2ZY

E: gram.infogovernance@nhs.scot (marked 'FAO DPO')

T: 01224 551549

Please note emails from your private email address may not be secure.

Your complaint will be acknowledged in no more than 30 days from receipt.

You may also wish to contact the Information Commissioner's Office - <https://ico.org.uk/for-the-public/how-to-make-a-data-protection-complaint/> - or seek to enforce your rights via judicial remedy.

If you wish to make a broader complaint, for example about the service you have received, please contact the Feedback and Complaints Service - <https://www.nhsgrampian.org/about-us/contact-us/feedback-and-complaints/>.