Southern Hampshire
PRIMARY CARE ALLIANCE

# IG Framework

1.1

| | |
|---|---|
| Document Type: | Policy & Procedure/Protocol/etc |
| Current Status: | Final/Draft/NEW |
| Version: | 1.1 |
| Reviewed by: | Lee Busher |
| Latest review date: | July 2022 |
| Document Owner: | Sue Williams |
| This version approved: | MM YYYY |
| Next review due: | July 2024 |
| Approved by | Firstname Secondname |
| Original publication date | DD 11 2020 |
| Applies to: | e.g. All Southern Hampshire Primary Care Alliance Staff/Clinical Staff/etc… |

**Version Control**

| Version | Date | Author | Change Summary |
|---|---|---|---|
| **1.1** | 21/07/2022 | L Busher | Formatting changes and review |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Contents

## 1. INTRODUCTION

As a provider of NHS services Southern Hampshire Primary Care Alliance (SHPCA) maintain an Information Governance Management Framework (IGMF) which demonstrates the robust nature of SHPCA's treatment of information governance. SHPCA complete and publish the NHS Data Security and Protection Toolkit (DSPT) annually.

SHPCA commit to high standards of information governance requiring clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources in alignment with Data Protection legislation including GDPR and the 10 Data Security Standards. SHPCA demonstrate our compliance in delivering these requirements and our IG management framework within our DSPT submissions. The framework is approved at senior management level and reviewed regularly.

This strategy sets out the plan and the approach to be taken to provide robust information governance (IG) for the future management of information. Using the Data Security and Protection toolkit as its foundation the strategy focuses on setting standards and implementing these.

## 2. SCOPE AND DEFINITIONS

The IGMF is a documented approach to the organisation and delivery of clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

This document applies to all directly and indirectly employed staff within SHPCA and other persons working within or on behalf of the organisation. This document applies to all third-party contractors or those with similar relationships through their contractual agreement with SHPCA.

'Information governance' describes the approach taken within which information standards are developed, implemented, and maintained by SHPCA and ensures best practice applies in particular to all information relating to the organisation and individuals.

Information governance management ensures that data is sourced, held and used legally, securely, efficiently and effectively, in order to deliver the best possible care in compliance with legislation and advice received from bodies including NHS Digital. Information is a vital asset to the organisation supporting the effective management of commissioned services and resources. Therefore, it is essential that all organisational information be managed effectively within a robust information governance management framework.

The organisation requires accurate, timely and relevant information to enable it to provide the highest quality healthcare and to operate effectively and meet its objectives. It is the responsibility of all staff to ensure that information is accurate and current and is used proactively in the conduct of its business. Accurate information that is dependable plays a key role in both corporate and clinical governance, strategic risk, performance management and service planning.

In order to assist staff with understanding their responsibilities under this strategy, the following types of information and their definitions are applicable in all SHPCA policies and documents.

| | |
|---|---|
| Personal Data (derived from the GDPR) | Any information relating to an identified/identifiable person ('data subject'); an identifiable individual is one who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person |
| 'Special Categories' of Personal Data (derived from the GDPR) | 'Special Categories' of Personal Data consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life |
| Personal Confidential Data | Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified/identifiable individuals, which should be kept private or secret. The definition includes living and deceased people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013). |
| Commercially confidential Information | Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to SHPCA or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations. |

## 3. FRAMEWORK

| Heading | Requirement |
|---|---|
| Senior/Key Roles | Senior Information Risk Owner (SIRO)<br>Caldicott Guardian (CG)<br>IG Lead<br>Data Protection Officer (DPO) |
| Policies | HR & Confidentiality Policies |
| Governance Bodies | Combined Assurance Group<br>(escalation to Board) |
| Governance Framework | Details of how responsibility and accountability for IG is cascaded through the organisation |

| | |
|---|---|
| Training & Guidance | Staff Code of Conduct for all staff Data Security policies, Confidentiality agreements. Training for specialist IG roles |
| Incident Management | Documented procedures and staff awareness |

## 4. SENIOR ROLES

**Senior Information Risk Owner (SIRO)**

A member of the Senior Management Team (SMT) / Board with overall responsibility for the organisation's information risk treatment. The SIRO will also lead and implement the Information Governance risk assessment and advise the SMT on the effectiveness of risk management across the organisation. The SIRO's responsibility is formalised within a job description.

**Information Asset Owners (IAO)**

A senior member of staff who is the nominated owner for one or more of the identified information assets of SHPCA. The IAO responsibility is formalised within a job description.

**Information Governance (IG) Lead**

A senior representative in the organisation who leads and co-ordinates the IG work programme. This may be the same individual as the SIRO.

**Caldicott Guardian (CG) (advisory, not accountable)**

A member of the SMT and a senior health or social care professional, responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing. This may not be the same individual as the SIRO and IG Lead.

**The Data Protection Officer (DPO)**

Reports directly to the Board in matters relating to data protection assurance and compliance, without prior oversight by their line manager. The DPO must ensure that their responsibilities are not influenced in any way and should a potential conflict of interest arise report this to the highest management level.

The DPOs cannot hold a position within the organisation that can be considered a key decision maker in relation to what personal data is collected and used. Their primary duties are to

- Inform and advise organisation and staff of their IG responsibilities
- Monitor compliance with the GDPR and the DPA 2018
- Provide advice where requested regarding the Data Protection Impact Assessment, and monitor performance
- Cooperate and provide a contact point with the Information Commissioners Office
- Ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects that the ICO is informed no later than 72 hours after the organisation becomes aware of the incident

They must give due regard to the risks associated with the processing of data undertaken by the organisation and work with the SIRO and Caldicott Guardian to achieve this.

## 5. POLICIES

These set out scope and intent. The IG and IT security policies are reviewed by key IG/IT roles as appropriate and agreed at Director level. Policies are reviewed annually or earlier where a change to national guidance or working practices is found. Policies include clear version controls.

A list of policies is provided at Annex A

## 6. GOVERNANCE BODIES

SHPCA's Combined Assurance Group will be the mechanism for directing and approving IG work programmes, receiving reports and assessing policies. The IG experts meet regularly (maximum of weekly) to share learning and best practice and to ensure IG work programmes are on track, particularly the DSP Toolkit plans and submissions.

Membership of this meeting typically includes the Chief Executive Officer (COO), SIRO, CG and DPO plus additional key members of staff.

Any items for escalation are taken to the monthly Board meeting unless an extraordinary meeting is required earlier.

## 7. GOVERNANCE FRAMEWORK

The contracts of all SHPCA staff include specific confidentiality and data protection clauses. IG Confidentiality Agreements are signed separately. Data Security Awareness training is completed by all staff and further in-house IG training is available.

## 8. DATA PROTECTION & SECURITY TOOLKIT (DSPT)

The DSPT standards have been achieved by SHPCA since 2018. SHPCA will continue to measure our performance against the data security national standards as set out in the Data Security and Protection Toolkit. Matters relating to the completion of the DSPT will be brought to the Combined Assurance Group.

## 9. IG TRAINING AND GUIDANCE

All staff receive IG training during their induction process with SHPCA and annual mandatory renewal training. Additional training is given by the DPO (during IG induction meeting where possible) and within team meetings and or team events. Statutory and mandatory training is tracked and expiry notified to individuals, additional monitoring ensures statutory and mandatory training is renewed. Timely reminders of data and IG security are issued as necessary by the DPO/CG at team meetings and via electronic methods.

SHPCA policies are held on the SHPCA One Drive and accessible via the Staff Portal (intranet).

The SHPCA induction process has been developed to ensure all staff understand the policies relevant to their work and their importance in shaping the way SHPCA include IG security and processes by design and default.

## 10.INCIDENT MANAGEMENT

Guidance has been issued to staff on actions to be taken in the event of IG incidents e.g. data loss, breach of confidentiality and IT security incidents e.g. loss or theft of a laptop. Any incident is reported to the DPO, CG, SIRO or IG Lead immediately and with reference to at least one further member of the senior IG staff, a decision is reached as to what actions need to be taken and whether the incident is reportable to the ICO; this is completed withing the 72 hour statutory limit. All data security incidents or near misses are collated in the Data Security Breach log. SHPCA further records clinical and non-clinical incidents using the Quasar platform which is recognised by the Clinical Commissioning Group and local General Practice.

Incidents are brought to the Combined Assurance Group for discussion and escalated to the Board as necessary.

In the event of any incident the requirement for further training /changes to procedures will be assessed.

## 11.INFORMATION SHARING

SHPCA will actively engage with other organisations e.g. health organisations, police, councils where there is a clear need and where this is in line with legislation.

Where this activity is not covered by legislation, SHPCA will engage specific information sharing protocols such as Data Sharing Agreements and where necessary by direct patient consent.

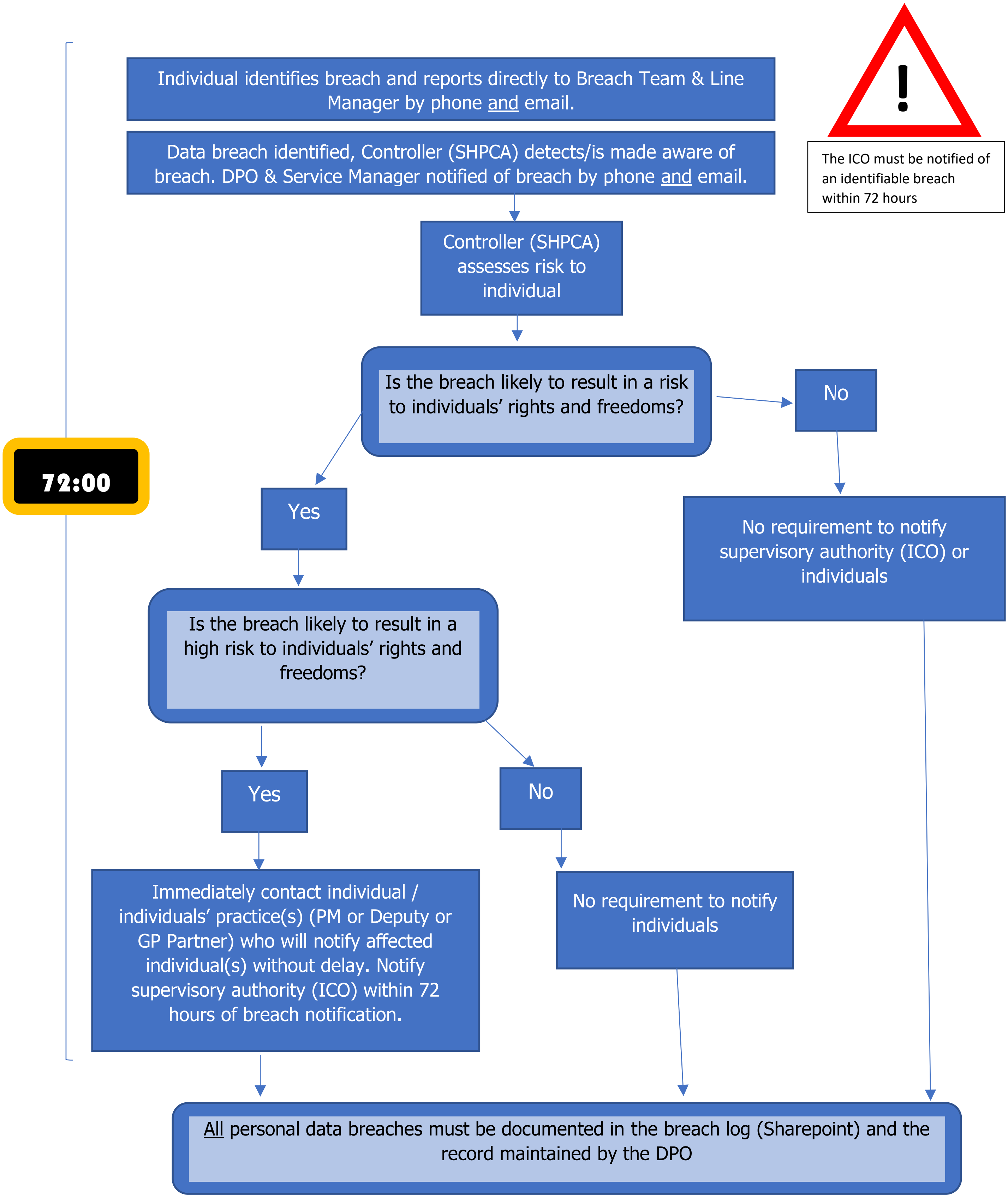
SHPCA maintain a list of its suppliers that handle personal information and the nature of that information, this is documented within the Information Asset Register. All contracts with third parties that handle personal information are compliant with ICO guidance. Providers of IT systems are vetted for appropriate certification.

## 12.APPENDIX A: POLICY LIST (INCLUDING BUT NOT LIMITED TO)

| **Does the policy/guidance affect one group less or more favourably than another on the basis of :** | Yes / No |
|---|---|
| Race | No |
| Ethnic origins | No |
| Nationality | No |
| Gender | No |
| Culture | No |
| Religion or belief | No |
| Sexual orientation including gay, lesbian, bisexual and transexual people | No |
| Age | No |
| Disability | No |
| **Is there evidence that some groups are affected differently?** | No |
| **If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?** | No |
| **Is the impact of the policy/guidance likely to be negative?** | No |
| **If so, can the impact be avoided?** | n/a |
| **What alternatives are there to achieving the policy/guidance without the impact?** | n/a |
| **Can we reduce the impact by taking different action?** | n/a |

| |
|---|
| 4C's Procedure (Complaints, concerns, incidents and compliments) |
| Caldicott Guardian Protocol |
| Code of Conduct |
| Computer, Email and Internet Use |
| Confidentiality of Patient Data |
| Declaration of Interest |
| IG Data Breach Risk Register |
| Data Protection & GDPR |
| Data Protection Impact Assessment |
| DSP Toolkit |
| IG Handbook |
| Password Policy |
| Privacy Policy |
| Retention & Erasure Guidelines |
| Sharing & Disclosure of Patient Information |
| Staff Agreement Form |
| Subject Access Request |
| Telephone Usage |

## 13.APPENDIX B: DATA BREACH FLOW CHART



Individual identifies breach and reports directly to Breach Team & Line Manager by phone and email.

Data breach identified, Controller (SHPCA) detects/is made aware of breach. DPO & Service Manager notified of breach by phone and email.

Controller (SHPCA) assesses risk to individual

Is the breach likely to result in a risk to individuals' rights and freedoms?

No

No requirement to notify supervisory authority (ICO) or individuals

Yes

Is the breach likely to result in a high risk to individuals' rights and freedoms?

Yes

Immediately contact individual / individuals' practice(s) (PM or Deputy or GP Partner) who will notify affected individual(s) without delay. Notify supervisory authority (ICO) within 72 hours of breach notification.

No

No requirement to notify individuals

All personal data breaches must be documented in the breach log (Sharepoint) and the record maintained by the DPO

The ICO must be notified of an identifiable breach within 72 hours