Data breach policy

Version control	Date and updates
Original	6 November 2019 (author: Dr G Schembri)
Version 2	21 September 2021 (updated DPO and LIO)
Version 3	7 June 2022 (no changes)
Version 4	New charity registered address (1 August 2022)
	Review August 2023

1. Introduction
   1.1. The British HIV Association (the 'Association') subcontracts several third-party organisations to collect, hold, processes, and share personal data on its behalf. Third party processor agreements are in place which includes the obligation to keep both personal and institutional data secure.
   1.2. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.
   1.3. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

2. Purpose and Scope
   2.1. The organisations subcontracted by the Association as data processors are obliged under Data Protection legislation to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.
   2.2. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents affecting the Association.
   2.3. This policy relates to all personal and special categories (sensitive) data regardless of format.
   2.4. The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

3. Definitions/Types of breach
   3.1. For the purpose of this policy, data security breaches include both confirmed and suspected incidents.
   3.2. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the Association's information assets and/or reputation.
   3.3. An incident includes but is not restricted to, the following:
      3.3.1. loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g., loss of laptop, USB stick, iPad/tablet device, or paper record);
      3.3.2. equipment theft or failure;
      3.3.3. system failure;
      3.3.4. unauthorised use of, access to or modification of data or information systems;
      3.3.5. attempts (failed or successful) to gain unauthorised access to information or IT system(s);
      3.3.6. unauthorised disclosure of sensitive/confidential data;
      3.3.7. website defacement;
      3.3.8. hacking attack;
      3.3.9. unforeseen circumstances such as a fire or flood;
      3.3.10. human error;
      3.3.11. 'blagging' offences where information is obtained by deceiving the organisation who holds it.

4. Reporting an incident
   4.1. Any individual who accesses, uses or manages the Association's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (DPO) (Chair, BHIVA External Relations Subcommittee) and IT Services (Netsynergy Ltd).

4.2. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.
4.3. The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (refer to Appendix 1).
4.4. All staff should be aware that any breach of Data Protection legislation may result in the Association's Disciplinary Procedures being instigated.

5. Containment and recovery
5.1. The Data Protection Officer will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.
5.2. An initial assessment will be made by the DPO in liaison with relevant officer(s) to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DPO).
5.3. The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.
5.4. The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.
5.5. Advice from experts may be sought in resolving the incident promptly.
5.6. The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment
6.1. An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered/reported.
6.2. The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.
6.3. The investigation will need to consider the following:
6.3.1. the type of data involved;
6.3.2. its sensitivity;
6.3.3. the protections are in place (e.g. encryptions);
6.3.4. what has happened to the data (e.g. has it been lost or stolen;
6.3.5. whether the data could be put to any illegal or inappropriate use;
6.3.6. data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
6.3.7. whether there are wider consequences to the breach.

7. Notification
7.1. The LIO and/or the DPO, in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.
7.2. Every incident will be assessed on a case by case basis; however, the following will need to be considered:
7.2.1. whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation
7.2.2. whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
7.2.3. whether notification would help prevent the unauthorised or unlawful use of personal data;
7.2.4. whether there are any legal/contractual notification requirements;
7.2.5. the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

7.3. Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks.
Individuals will also be provided with a way in which they can contact the Association for further information or to ask questions on what has occurred.

7.4. The LIO and/or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7.5. The LIO and or the DPO will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

7.6. A record will be kept of any personal data breach, regardless of whether notification was required.

8. Evaluation and response

8.1. Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

8.2. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8.3. The review will consider:

8.3.1. where and how personal data is held and where and how it is stored;

8.3.2. where the biggest risks lie including identifying potential weak points within existing security measures;

8.3.3. whether methods of transmission are secure; sharing minimum amount of data necessary;

8.3.4. staff awareness;

8.3.5. implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

8.4. If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by Association Executive Committee.

9. Policy Review

9.1. This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

9.2. This policy was last reviewed in May 2018. The policy was approved by the Association Executive Committee in May 2018.

Appendix 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify the Association (email: bhiva@bhiva.org), complete Section 1 of this form and email it to the Data Protection Officer, Dr Matthew Page (email: matthewpage1@nhs.net) and IT Services (Netsynergy email: nick@netsynergy.co.uk), where appropriate.

Section 1: Notification of Data Security Breach To be completed by Person who discovered breach

Section 1: Breach notification	
Name of person reporting incident:	
Date form completed:	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Contact details of person reporting incident	
Brief description of incident or details of the information lost	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken so far	
For use by Data Protection Officer:	
Received on:	
Received from:	
Sent to:	
Sent on:	
Further action taken:	

Section 2: Assessment of Severity To be completed by the Lead Investigation Officer in consultation with BHIVA, Medivents and Netsynergy as appropriate

Section 2: Assessment of severity	
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? Any backups available?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the Association or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data ▪ Special categories personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
Detailed profiles of individuals	
Security information that could compromise the safety of individuals if disclosed.	
Sensitive institutional information	
Data Protection Officer and/or Lead Investigation Officer to consider whether it should be escalated to the appropriate Association Executive Committee member	

Section 3: Action taken To be completed by Data Protection Officer and/or Lead Investigation Officer/BHIVA or affected stakeholders

Section 3: Action	
Incident number	e.g. 001
Date:	
Action taken by responsible officer/s:	
Was incident reported to Police? If yes, enter date police notified and any follow up action	
Was incident reported to internal and other affected stakeholders? If yes, enter date they were notified and any follow up action	
Notification to the Information Commissioner's Office (ICO), if required. If yes, enter date and details:	
Notification to affected individuals (if required). If yes, enter date and details:	
Other notifications required:	

Notification to the ICO

Not all personal data breaches have to be notified to the ICO. The breach will only need to be notified if it is likely to result in a risk to the rights and freedoms of data subjects, and this needs to be assessed by the Company on a case-by-case basis. A breach is likely to result in a risk to the rights and freedoms of data subjects if, for example, it could result in:

- loss of control over their data
- limitation of their rights
- discrimination
- identity theft
- fraud
- damage to reputation
- financial loss
- unauthorised reversal of pseudonymisation
- loss of confidentiality
- any other significant economic or social disadvantage.

Where a breach is reportable, the Company must notify the ICO without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If our report is submitted late, it must also set out the reasons for our delay. Our notification must at least include:

- a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records
- the name and contact details of the Company's CEO
- a description of the likely consequences of the breach
- a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.