Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach then please notify the Data Protection Officer (DPO) and Senior Management immediately via email and telephone.

It is extremely important that all employees report breaches promptly since our organisation is required to formally notify the Information Commissioners Office (ICO) of the data breach within 72 hours of the breach date / time under the General Data Protection Regulations (GDPR).

Please note it is the responsibility of the Data Protection Officer (DPO) and Senior Management to formally investigate the breach and inform the relevant bodies if required.

Please complete this form to the best of your abilities giving as much information as possible to make an initial assessment.

Failure to notify a data breach in a timely fashion may result in disciplinary action

Steps to take:

1. Call the office and speak to the Data Protection Officer on 01903 703 270
2. Complete section 1 of this form and email it to [itsupport.sussexcds@nhs.net](mailto:itsupport.sussexcds@nhs.net)

What Happens Next:

The Data Protection Officer (DPO) will complete the remainder of the form (Section 2) and investigate further. Data breaches concerning NHS services will then be reported through the Breach Reporting tool of the Data Security and Protection Toolkit to the relevant bodies or via email / online submission to the ICO in the case of private services as required.

For more information about how data breaches are managed, please see our Data Breach Policy and Incident Reporting Framework.

# Section 1: Notification of Data Security Breach

To be completed by the employee reporting the incident.

|  |  |
| --- | --- |
| **Name of employee reporting the incident** |  |
| **Contact details of employee reporting the incident (email address, telephone number)** |  |
| **Date incident was discovered** |  |
| **Date(s) on which the incident occurred** |  |
| **Place of incident** |  |
| **Brief description of the incident and details of any data lost** |  |
| **Number of Data Subjects (Patient Records/ Staff Records) affected, if known.** |  |
| **Has any personal data been placed at risk? If so then please provide details.** |  |
| **Brief description of any action(s) taken at the time of discovery.** |  |
| ***For use by the Data Protection Officer*** | |
| **Received by** |  |
| **Received at (date and time)** |  |
| **Forwarded for action to** |  |
| **Forwarded at (date and time)** |  |

# Section 2: Assessment of Severity

To be completed by the Lead Investigation Officer in consultation with employees and if appropriate the IT Team.

|  |  |
| --- | --- |
| **Details of any IT systems, equipment, devices or records involved in the breach** |  |
| **What is the nature of the data lost?** |  |
| **How much data has been lost?** |  |
| **If a laptop is lost / stolen then how recently was the laptop backed up onto central IT systems?** |  |
| **Is the information unique? Will its loss have adverse operational, research, financial, legal, liability or reputational consequences for the Organisation 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 data that fall into the following categories.** |  |
| **HIGH RISK personal data**  **Special category personal data relating to an individual’s:**   1. **Racial or ethnic origin;** 2. **Political opinions or religious beliefs;** 3. **Genetics;** 4. **Biometrics;** 5. **Health;** 6. **Sex life or sexual orientation.** |  |
| **Information that could be used to commit identify fraud such as; personal bank account or other financial information; national identifiers such as NI number or copies of passports and visas.** |  |
| **Personal information relating to vulnerable adults and children.** |  |
| **Security information that would compromise the safety of individuals if disclosed.** |  |

# Section 3: Action Taken

To be completed by the Data Protection Officer and / or the Lead Investigation Officer

|  |  |
| --- | --- |
| **Incident Number** |  |
| **Report received by** |  |
| **Report received at (date and time)** |  |
| **Action taken by responsible officers(s)** |  |
| **Was the incident reported to the police?** | YES / NO |
| **If YES, notified at (date and time)** |  |
| **Follow up action required / recommended** |  |
| **Reported to Data Protection Officer and Lead Investigation Officer at (date and time)** |  |
| **Reported to other internal stakeholders (details, dates and times)** |  |
| **Notification to ICO** | YES / NO |
| **If YES, notified at (date and time)** |  |
| **If YES, details** |  |
| **Notification to Data Subjects** | YES / NO |
| **If YES, notified at (date and time)** |  |
| **If YES, details** |  |
| **Notification to other external regulators / stakeholders** | YES / NO |
| **If YES, notified at (date and time)** |  |
| **If YES, details** |  |