Information Breach Notification Form

This form is to be completed in line with the mandated requirements in the [Information Breach Policy](https://ww2.health.wa.gov.au/About-us/Policy-frameworks/Information-Management/Mandatory-requirements/Access-Use-and-Disclosure/Information-Breach-Policy) and reference to the mandatory information in the [Information Breach Response Standard](https://ww2.health.wa.gov.au/~/media/Files/Corporate/Policy-Frameworks/Information-management/Policy/Information-Breach-Policy/Supporting/Information-Breach-Process-Guide.pdf).

**Part 1- Information Breach Report**

**To be completed by the person who identified the breach and then submitted to their line manager, or as directed by local procedure for further action.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Details of the employee member reporting the breach incident.** | | | | | | | | |
| Full name |  | | | | | |
| Position title |  | | Location/Department | |  | |
| E-mail |  | | Contact phone number | |  | |
| Line Manager |  | | Manager Notified | | Yes | No |
| **Details of the breach incident.** | | | | | | | | |
| Location | *Division/HSP/WA health entity where the breach occurred* | | | | | | |
| Date identified | *Date reporter became aware of the breach* | Date when it happened | | Click or tap to enter a date. | | | |
| What is the Information Asset? | *Name/Type of Information Asset. E.g. WebPAS, Medical Record, Personnel Records or External Information Asset.* | | | | | | |
| Information asset Custodian. Refer to: [WA health system Information Register](https://doh-healthpoint.hdwa.health.wa.gov.au/directory/Purchasing%20and%20System%20Performance/Data%20and%20information/Lists/WA%20health%20system%20Information%20Register/AllItems.aspx?PageView=Shared&InitialTabId=Ribbon.WebPartPage&VisibilityContext=WSSWebPartPage) |  | Custodian contacted | | Yes | | No | |
| Date contacted | | Click or tap to enter a date. | | | |
| Information Breach Category. Refer to Information Breach Standard. *Multiple boxes can be selected.* | Information System, Cyber Security | Health or Personal Information | | External Information Asset | | | |
| Corporate, financial, or workforce | Environmental or Physical | | All Apply | | | |

| **Description of the breach – Provide a brief and factual information only to inform assessment.** | |
| --- | --- |
| What happened? | *Example: Personal Information about a patient’s was accessed in WebPAS and provided to a relative.* |
| What format was the information received in? | *This information is intended to provide context that will assist the assessment of the information breach.* |
| Who accessed or received the information? | *Accessed by and/or provided to who?* |
| Was the breach intentional? | *Unauthorised, Intentional or unintentional?* |
| Describe what information was affected. | *Include details such as the volume affected, identifiability, and whether the information related to patient(s) or corporate records. E.g. A report listing 100 patients’ details* |
| Who/What caused it? | *Initial known or assumed cause of the breach. This may differ to the confirmed cause after further investigation.* |
| Who has been notified of the incident? |  |
| Were there other witnesses to the incident? | *Provide details of other persons that were witnesses to the incident* |

# Part 2 - Information Breach Assessment & Resolution

**To be completed by the relevant Manager, Information Custodian or other applicable person assessing the breach.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Details of the individual undertaking the assessment of the breach incident.** | | | | |
| Full name |  | | |
| Position title |  | Location & Department |  |
| E-mail |  | Phone number |  |

| **Assessment** | | | | | |
| --- | --- | --- | --- | --- | --- |
| Date received | |  | Greater than 30 days required to investigate | Yes | No |
| Date commenced | |  |
| **Potential breach of discipline/code of conduct?** | | ***If yes immediately contact the relevant WA health system entity’s responsible area and comply with their instructions. This will be the Integrity Unit, Human Resource/Workforce Unit, or other responsible area as per local policy and/or procedure.*** | | | |
| **Yes** | **No** |
| **Cyber security breach?** | | ***If yes immediately contact Health Support Services ICT helpdesk: 134477 or email: infosec@health.wa.gov.au and comply with their instructions.*** | | | |
| **Yes** | **No** |
| Who is affected by the information breach? | | *(e.g. staff, patients, general public, other government agencies, any third party).*  *The assessment may include reviewing whether individuals/organisations have been affected by the breach.* | | | |
| Who has been notified of the breach? | | *Other stakeholders/authorities/individuals. Record who and date notified.* | | | |
| What immediate actions were taken to contain the breach? | | *What was done to manage the risk of further damage/harm?*   * *Has the information been recovered?* * *Security measures taken.* | | | |
| What caused it?  Identify the causal factors and underlying causal circumstances. | | *The assessment may include reviewing:*   * *How did the current controls fail to mitigate the risk of breach?* * *Whether the breach occurred as part of a deliberate act or negligence.* * *Was it a one-off incident or does it expose a more systemic vulnerability?* | | | |
| What is the potential harm to the affected individuals or the organisation? | | *Consider the level of sensitivity of the information and what possible use there is for the information. For example, could it be used for identity theft, threats to physical safety, financial loss, or damage to reputation?*  *Is it Official information that could result in damage to individuals, organizations’ or government if released*  *Whether any individuals have personal circumstances which may put them at particular risk of harm.* | | | |
| What controls were in place to mitigate the risk of this information breach? | | *For example**: Policy, Procedures, Restricted Access, Monitoring, Security etc.* | | | |

|  |  |  |
| --- | --- | --- |
| **Review & Risk Management** | | |
| Is further investigation considered necessary and if so, how will this be undertaken? | *Will the breach need to be escalated or transferred to another authority?* |
| Risk Assessment. Refer to [WA health risk assessment tables](https://ww2.health.wa.gov.au/~/media/Files/Corporate/Policy-Frameworks/Risk-Compliance-and-Audit/Policy/WA-Health-Risk-Management-Policy/supporting/WA-risk-analysis-tables.pdf) | *Consider: Individual harm, financial loss, service interruption, reputational damage. Assess:*   * *The likelihood and consequence should the breach recur.* * *The controls managing the risk* * *Risk acceptance/tolerance.* | |
| After looking at the WA health risk assessment tables, what is the level of risk for the most impacted category? | * *1 Insignificant* * *2 Minor* * *3 Moderate* * *4 Major* * *5 Catastrophic* | |
| Treatment Action Plan (TAP) - What is required to prevent the breach from occurring again? | *The TAP may include:*   * *Strengthening the current controls and any additional controls that have been developed/implemented.* * *Improving security and access.* * *Education and training* * *Changing the Environment or Location* | |

|  |
| --- |
| **Summary** |
| *Summary of breach, may include status of:*   * *Actions completed* * *Information disclosed/recovered* * *Ongoing Investigation* * *Further risks* * *Risks accepted or outstanding* |

*On completion, please forward this form to* [RoyalSt.PSPInfoManagement@health.wa.gov.au](mailto:RoyalSt.PSPInfoManagement@health.wa.gov.au)