|  |
| --- |
| Healthcare entities must inform the Department of Health (‘’DOH’’) about the personal data breach. The data protection representative from the healthcare entity must report the personal data breach to DOH on behalf of the healthcare entity.  The healthcare entity shall provide the following information to DOH:   * Nature of the personal data breach; * Approximate number of impacted records and data subjects; * Consequences of the personal data breach; * Measures taken to address the personal data breach, and the mitigation plan; * Additional documents and/or information related to the personal data breach, and the remedial actions taken; * Name and contact details of the data protection representative of the healthcare entity, where further information can be obtained from.   Reporting personal data breaches to the Department of Health can be done via dataprivacy@doh.gov.ae. You will be provided with a personal data breach form.  The Department of Health will review the report and may contact you for clarification or further information. If the data breach is considered to be minor in terms of risk of harm to the data subjects whose data has been breached and/or demonstrate that you are adequately implementing measures to mitigate the risk and prevent occurrences, then it may result in no further action.  Healthcare entities must notify the Department of Health of personal data breaches no later than 72 hours after becoming aware of the data breach. The healthcare entities must document all personal data breaches and provide the Department of Health with the requested information within 30 working days after the initial reporting.  When the personal data breach is likely to result in high risk to the data subjects, the healthcare entity must inform the data subject of the personal data breach in a clear and plain language and should include recommendations to mitigate any adverse effects.  The entity is required to complete the "Data Information Breach Form" in addition to submitting incident notifications and updates.  **Overview of the personal data breach** |

|  |  |
| --- | --- |
| Nature of the breach |  |
| Date of when the incident occurred |  |
| Date of when the incident was acknowledged |  |
| Date of when the incident was reported to DoH |  |
| Summary of the incident |  |
| How did the incident happen? |  |
| Reason for the delay in reporting the incident to DoH, if applicable |  |

**Impacted *PII and PHI***

|  |  |
| --- | --- |
| Details of the impacted PII and PHI |  |
| Number of impacted records |  |
| Number of impacted individuals |  |
| Have the impacted individuals been notified about this incident? |  |
| Potential detriment this incident will cause to individuals |  |
| Have any of the impacted individuals complained to the entity? |  |
| Has the entity taken any action by mitigating/minimizing the effect on the impacted individuals? |  |
| What are the steps taken by the entity to prevent the incident from occurring again? |  |

**Data Processors (Third-Party)**

|  |  |
| --- | --- |
| Was this incident a result of a data breach by a data processor? If not, please go to the next section. |  |
| What action(s) did the data processor take to mitigate the effect on the impacted individuals? |  |
| Were there any contractual obligation(s) with the data processor regarding the use of PII and PHI? |  |
| Did the contractual obligation(s) include technical and organizational security measures? |  |
| Do you consider the incident has breached any contractual obligations? |  |
| What action have you taken in regard to the processor? |  |

**Training & Guidance**

|  |  |
| --- | --- |
| As a data controller, were the employees at the entity trained on data protection and the appropriate regulations? |  |
| Is the training mandatory for all employees? |  |
| Did the employees, who are involved in this incident, complete the training? |  |
| As the data controller, have you provided a guideline or guidance to employees on how to handle PII and PHI that is related to this incident? |  |

**Reporting**

|  |  |
| --- | --- |
| Have you reported a PII and PHI breach to DoH in the past two years? |  |