Data Breach Considerations Worksheet

This worksheet is provided to facilitate a conversation about an agency’s data breach policies. Each consideration is listed and includes the corresponding section of the Data Breach Policy Template. Notes/status updates and draft language can be recorded in the columns provided. Once applicable considerations are addressed, teams may transfer their answers to the Data Breach Policy Template to facilitate completion of their data breach policy.

| Data Breach Policy Considerations Worksheet | | | |
| --- | --- | --- | --- |
| Considerations | Template Section | Notes /Status | Draft Language |
| **1. Data Breach Response Policy: Scope** |  |  |  |
| 1. How does this policy align with any existing state policy and/or broader state agency data breach response policies? | 2 and 4a |  |  |
| 1. What Part C/619 data are included and excluded by this data breach response policy? | 4b, 4c |  |  |
| 1. What constitutes an unauthorized release or access of personally identifiable information (PII) (e.g., unauthorized copying of data, system hacking, unauthorized data viewing, loss of flash drive or laptop with data)? | 3 |  |  |
| 1. Who must adhere to the data breach response policy (e.g., staff, participating agencies, vendors, contractors)? | 4d |  |  |
| 1. Are there binding clauses in contracts with vendors regarding data breach responsibilities? | 4c |  |  |
| 1. What data breach training exists for agency staff? | 5b |  |  |
| **2. Data Breach Response Policy: Responsibility** |  |  |  |
| 1. Who (what role) is responsible for informing Part C/619 staff and ensuring their compliance with the data breach response policy? | 5b, 6a |  |  |
| 1. If a Part C/Part B 619 data breach is suspected, who (what role) is responsible for investigating and confirming it? | 5b |  |  |
| 1. What team or individuals are responsible for authorizing and carrying out the actions of the data breach response? | 5b |  |  |
| 1. What monitoring/tracking will occur to ensure policy compliance? What monitoring documentation is needed? | 5b |  |  |
| **3. Data Breach Response Policy: Data Breach Immediate Actions** |  |  |  |
| 1. Who (what role) reports a Part C/619 data breach to administration? | 6a |  |  |
| 1. When shall a data breach be reported internally? | 6b |  |  |
| 1. Under what circumstances shall a data breach be reported to individuals potentially at risk? | 6c |  |  |
| 1. Under what circumstances shall a data breach be publicly reported? | 6c, 6d |  |  |
| 1. How should a data breach be reported to those at risk? To the public? | 6d |  |  |
| 1. When will individuals and/or public be notified? | 6d |  |  |
| 1. Who (what role) will notify individuals and/or public about the data breach? | 6d |  |  |
| **4. Data Breach Response Policy: Post Breach Actions** |  |  |  |
| 1. Under what circumstances will sanctions/consequences be levied on those responsible for the Part C/Part B 619 data breach? | 7a |  |  |
| 1. What procedures will be taken to prevent similar data breaches in the future (e.g., investigation, process review, training, security measures)? | 7c |  |  |
| 1. What are the projected timeline and process for implementing these response procedures? | 7b |  |  |