# Narrative Description of Privacy Program

The Responder must provide a description of its privacy program using the following topic headings. In this section, the terms “data” or “sensitive data” includes Protected Health Information (PHI) and private information about Enrollees, but does not include commercially non-public data, provider data, or personnel data.

A page limit of one page per topic or subtopic is recommended. Examples of policies/procedures, required formats for data requests, Business Associate Agreements (BAAs), training materials or similar helpful documents may be attached as exhibits only if referred to in the narrative. Trade secret data should be clearly marked on every page. Exhibits are not required.

Please provide a narrative covering the following topics and subtopics:

1. Sensitive Data That Must Be Protected -- describe which data are protected, and under which laws the Responder protects sensitive data.
2. Methods, Policies and Steps Taken to Protect Sensitive Data – describe each of the following:
   1. Legal agreements (with whom, how often reviewed or renewed, and what sensitive data are covered)
   2. Training (of whom, when required, on which data privacy topics, and how often the materials are reviewed or updated)
   3. Ongoing Training (of whom, when required, on which data privacy topics, and how often reviewed or updated)
   4. Physical security methods for protecting sensitive data in media other than data in computer systems, such as paper, printing, or portable drives. (Computer system security is described in the “Vendor Security & Compliance Questionnaire” below).
3. Failures to Protect Sensitive Data – provide a general description of:
   1. What is the general chronological process for investigation
   2. To whom are data privacy incident and data breaches reported
   3. Escalation process for significant breaches of sensitive data
   4. Learning and planning process to improve failed systems.
4. Auditing of Procedures to Protect Sensitive Data -- describe the Responder’s auditing system:
   1. Who audits processes for sensitive data protection
   2. When are audits performed
   3. Learning and planning process to improve systems.

# Vendor Security & Compliance Questionnaire; Responder must complete the “MN-IT Vendor Security Compliance Questionnaire Form” available below and submit it with its Proposal. STATE’s Office of Information Security may ask for additional information from successful Responders based on this form.



# Listing of Sensitive Data Breaches – Data Dictionary and Examples

Responder must submit a spreadsheet or Word table using the following headings and inserting the text or value required. Brief descriptions are recommended. More significant breaches (for example, more persons affected or having a greater remediation cost) should be described more fully than smaller breaches.

Breaches to be listed include breaches of Health Insurance Portability and Accountability Act (HIPAA) (as defined under section 13.6.3.1 of the model contract in Attachment A) and Minnesota Government Data Practices Act (MGDPA) (as defined under section 13.6.4 of the model contract in Attachment A) in all Medicaid lines of business.

**List breaches in the past five years only (from 1/1/2016 through 12/31/2021)**. If the Responder does not currently have a Families and Children contract with the State or has not been doing business in Minnesota during this period, they should select a current market or product to use in the response for their list of breaches, including non-Medicaid information if Medicaid is not available.

| **Column number** | **Heading** | **Format** | **Contents** |
| --- | --- | --- | --- |
| A | Description | Free text | Brief description of the breach: what happened? Who caused the breach? |
| B | Medium | Free text | Examples: paper; mailing; verbal; e-mail; computer system access, etc. |
| C | Data type | Free text | Examples: personal identifiers, address, claims, diagnosis, pharmacy, billing, Social Security information. |
| D | Breach start date | Date | The date on which the breach first occurred. |
| E | Breach end date | Date | The date on which the breach was ended. |
| F | Length of breach | Number | Calculate (E minus D) |
| G | Discovery date | Date | The date on which the breach was discovered |
| H | Discovery length | Number | Calculate (G minus D)  In column M or as a note following this table, explain the delay in discovery for any breaches where the time between the breach start date and discovery was more than 30 days. |
| I | Number of persons affected | Number | Count of persons whose data was exposed |
| J | Date of notice | Date | Date of notice to the affected persons |
| K | Date of notice to DHS/OCR | Date | Date of notice to regulators, if required |
| L | Breach identifier | Number | Numeric identifier of the breach, used to link it to description in column “M,” if needed. |
| M | Actions taken | Free text | Brief description of the actions taken to mitigate the error or avoid repetition. Examples include retrieval of misdirected data, offer of credit monitoring, training, termination of subcontractor, new process or new verification procedure, additional auditing.  Because the space in a table is limited, longer descriptions may be included after the table in paragraph format, linking the table row to the paragraph with the number in column “L.” See example below. |

*Fictional examples* of data entered into data dictionary:

| A | B | C | D | E | F | G | H | I | J | K | L | M |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Description | Medium | Data type | Breach start date | Breach end date | Length of breach | Discovery date | Discovery length | Number of persons affected | Date of notice | Date of notice DHS/OCR | Breach identifier | Actions taken |
| A staff member may have impermissibly obtained a member's home phone number and address from an MCO system. | Systems access | Personal identifiers | 8/5/2019 | 8/5/2019 | 1 | 8/6/2019 | 1 | 1 | 8/12/2019 | NA | #19-186 | Terminated access to systems and employment. Free credit monitoring service was offered. |
| Business associate mailed a pre-treatment Estimate of Benefits to a member's former address. | Mail | Demo-graphic, diagnosis | 4/3/2019 | 6/2/2019 | 40 | 4/23/2019 | 20 | 1 | 4/25/2019 | NA | #19-277 | **See below.** |
| BA sent ID cards to wrong addresses |  |  | 2/6/2019 | 2/9/2019 | 3 | 2/9/2019 | 3 | 44 | 2/14/2019 | NA | #19-100 | Requested destruction of ID card from recipients. Audited BA’s processes for stuffing mailings. |

**Note on Breach # 19-277:** The individual who received the misdirected document was the member's former guardian/care giver. He reported the mailing error to the business associate and advised that he would destroy the document. The business associate updated their systems to reflect the correct mailing address. A new Estimate of Benefits was sent to the member's correct address. MCO worked with the member's county worker to update his address in DHS' system so that it would flow to MCO's system via the next monthly enrollment file.