



MEDICAID POLICY CLARIFICATION #PC000217.1 MANAGED CARE PLAN SECURITY INCIDENT PROCESS

July 23, 2024

To: Iowa Medicaid Managed Care Plans

This letter is a formal notification of the state's expectations related to the operations and implementation of Iowa Medicaid under the managed care program. This purpose of this letter is to do following:

- Provide formal guidance
- Clarification of existing Iowa Medicaid policy
- Guidance on new process or policy
- Request for information

Managed Care Plan (MCP) reporting requirements related to incidents and breaches of Protected Health Information (PHI)

For the purposes of this guidance, the following terms are used as follows:

- Privacy or Security Incident: Notification to the affected individuals is not required.
- Privacy or Security Breach: Notification to the affected individuals is required unless a Breach Notification Risk Assessment results in low probability of compromise.

Staffing and training duties of the MCP:

In order to streamline and expedite the incident reporting process, it is imperative each MCP takes the following steps:

- I. Appoint an MCP Liaison: The MCP Liaison is the dedicated individual responsible for the entire incident reporting process. This individual will:
 - a. Serve as the main point of contact for the Iowa Medicaid Health Insurance Portability and Accountability Act (HIPAA) Liaison.
 - b. Review the Iowa Department of Health and Human Service (HHS) Incident Report 470-5134, located at [Health Insurance Portability & Accountability Act | Health & Human Services \(iowa.gov\)](#), to ensure it is completed correctly and accurately and contains all of the necessary detail.
 - c. Ensure **all** required information and documentation is included. See the steps the MCP must complete immediately following this section below.

- d. Submit all incident reports and documentation per this policy clarification and the HHS Business Associate Agreement.
 - e. Respond timely to requests for additional information from the Iowa Medicaid HIPAA Liaison and gathers all additional materials as needed from the MCP incident reporters.
 - f. Submit updated HHS Incident Reports and documentation when the issue is initially reported as “under investigation.”
 - g. Track all incidents through completion.
2. Provide initial and any ongoing training to all staff involved in the incident reporting process regardless of role. The MCP will contact HHS if assistance with training is needed.
 3. Update the Iowa Medicaid HIPAA Liaison prior to a change in the appointment of the MCP Liaison.

When any confidential information of a Medicaid member or the social security number of a provider is exposed or disclosed to an unauthorized party, including another covered entity, by any means, **the MCP must** complete the following steps as outlined in the HHS Business Associate Agreement:

1. Complete the HHS Incident Report. All sections of this form must be completed with **detailed** information describing the incident/breach.
2. Send the completed HHS Incident Report to the Iowa Medicaid HIPAA Liaison at IMEHIPAALiaison@dhs.state.ia.us within three (3) business days of discovery of the incident/breach.
3. With the completed HHS Incident Report in step 2 above, send the following additional information to Iowa Medicaid at IMEHIPAALiaison@dhs.state.ia.us:
 - a. Documentation of the information involved which will vary depending on the circumstances. This includes, but is not limited to, a copy of the paper or electronic document, email, column headings of a spreadsheet or data file with all personal information redacted, description of lost or stolen equipment, etc.
 - b. Actual written attestation received from the unauthorized recipient indicating **all** of the following:
 - 1) Originals of the information were returned or destroyed.
 - 2) No copies of the information were made.
 - 3) The information was not further disseminated.

Note: If you cannot obtain written attestation, obtain verbal attestation and document the verbal attestation in the HHS Incident Report.
 - c. Breach notification: Include **one** of the following:
 - 1) Draft breach notification letter which must include all of the following:
 - i. Types of information disclosed (name, address, date of birth, state identification number, etc.),
 - ii. Specific measures being taken to resolve the issue that led to the incident,
 - iii. What the member can do to protect themselves from identity fraud, and
 - iv. Contact information for the MCP.

2. Breach Notification Risk Assessment indicating low probability of compromise. HHS will not accept a reference to a completed risk assessment mentioned in the HHS Incident Report. The MCP must submit the actual breach notification risk assessment.

Note: The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Specifically see §164.402(2) 2) Except as provided in paragraph (I) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- i. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
 - ii. The unauthorized person who used the protected health information or to whom the disclosure was made;
 - iii. Whether the protected health information was actually acquired or viewed; and
 - iv. The extent to which the risk to the protected health information has been mitigated.
4. When instructed to do so by the Iowa Medicaid HIPAA Liaison or ISPO, mail the Information Security and Privacy Office (ISPO)-approved breach notification letter to the impacted member or provider, and send the Iowa Medicaid HIPAA Liaison a copy of the signed breach notification letter once mailed.
 5. Initial HHS Incident Report – issue under investigation
 - a. In these instances, the MCP must submit the items in 3a. & 3b. above with the initial HHS Incident Report.
 - b. Unless otherwise agreed upon by the MCP and HHS, the MCP must submit an updated HHS Incident Report with the results of the investigation and the draft breach notification letter or breach notification risk assessment in 3c. above within five (5) business days of the submission date of the original HHS Incident Report.

The Iowa Medicaid HIPAA Liaison will take the following steps:

1. Review the completed HHS Incident Report. If additional information is needed, work with the MCP Liaison to get the necessary information.
2. Submit the HHS Incident Report and all other information received from the MCP Liaison to the HHS ISPO.

The ISPO will take the following steps:

1. Complete a separate investigation.
2. Review the breached information and determine the types of data elements compromised.
3. Determine if breach notification is required. If the MCP's determination is in conflict with the ISPO's determination, notify the Iowa Medicaid HIPAA Liaison to obtain the draft breach

notification letter from the MCP. Notification must be made as soon as possible but **no later than 60 days** from date of discovery of the breach.

4. Approve the breach notification letter and send it to the Iowa Medicaid HIPAA Liaison.
5. Log the incident/breach and maintain copies of all documents.
6. Report breaches to Health and Human Services, Office of Civil Rights (HHS/OCR).
7. Report the number of incidents and breaches to HHS management.

After ISPO has completed the above steps, the Iowa Medicaid HIPAA Liaison will do the following:

1. Inform the MCP if the ISPO determines breach notification is required when the determination is in conflict with the MCP's determination.
2. Return the breach notification letter to the MCP Liaison after it is approved by the ISPO, when appropriate.
3. Schedule meetings between the Iowa Medicaid, the MCP, the ISPO, and the Assistant Attorney General if the MCP has questions regarding their incidents/breaches, the need for breach notification, etc.
4. Send the ISPO a copy of the signed breach notification letter sent to the member or provider.

Related Policy Clarifications:

This policy clarification should be used in correlation with the following policy clarifications:
Replaces PC000217

This formal guidance impacts capitation rates in the following manner:

- This [is was] an Iowa Medicaid practice prior to April 1, 2016 and was included in the experience used to develop the capitation rates.
- This is a new process or policy that does not have a fiscal impact.
- This is a new process or policy that will be reflected in revised capitation rates and implemented July 1, 2021.

The managed care plans shall implement this guidance immediately. The department will monitor progress towards implementation and may impose remedies for failure to implement.