

Policy Clarification #000306

Reporting Requirements Related to Incidents and Breaches of Protected Health Information (PHI)

January 23, 2026

To: Iowa Medicaid Managed Care Plans

This letter is a formal notification of the Department's expectations related to the operations and implementation of Iowa Medicaid under the managed care program.

Purpose of this communication (check all that apply):

- ☒ Provide formal guidance
- ☒ Clarification of existing Iowa Medicaid policy
- ☐ Guidance on new process or policy
- ☐ Replacement of prior PC: [PC #]

The purpose of this letter is to provide **Managed Care Plans (MCP)** guidance on reporting requirements related to incidents and breaches of Protected Health Information (PHI).

Staffing and training duties of the MCP:

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

1. 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 Department of Health and Human Services (Iowa HHS) Incident Report 470-5134, located at <https://hhs.iowa.gov/hipaa> Business Associate Agreement, to ensure it is completed correctly and accurately and contains all of the necessary details.
 - 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 Iowa HHS Business Associate Agreement.
 - e. Respond timely to requests for additional information from the Iowa Medicaid HIPAA Liaison and gather all additional materials as needed from the MCP incident reporters.
 - f. Submit updated Iowa 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 Iowa 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 Iowa HHS Business Associate Agreement:

1. Complete the Iowa HHS Incident Report. All sections of this form must be completed with **detailed** information describing the incident/breach.
2. Send the completed Iowa HHS Incident Report to the Iowa Medicaid HIPAA Liaison at imehipaaliaison@hhs.iowa.gov within three (3) business days of discovery of the incident/breach.
3. With the completed Iowa HHS Incident Report in step 2 above, send the following additional information to Iowa Medicaid at imehipaaliaison@hhs.iowa.gov:
 - 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** the following:

- i. Originals of the information were returned or destroyed.
- ii. No copies of the information were made.
- iii. The information was not further disseminated.

Note: If you cannot obtain written attestation, obtain verbal attestation and document the verbal attestation in the Iowa HHS Incident Report.

- c. Breach notification: Include **one** of the following:

- i. Draft breach notification letter which must include all of the following:
 1. Types of information disclosed (name, address, date of birth, state identification number, etc.),
 2. Specific measures being taken to resolve the issue that led to the incident,
 3. What the members can do to protect themselves from identity fraud, and
 4. Contact information for the MCP.
- ii. Breach Notification Risk Assessment indicating low probability of compromise. Iowa HHS will not accept a reference to a completed risk assessment mentioned in the Iowa 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) - Except as provided in paragraph (1) 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:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
 2. The unauthorized person who used the protected health information or to whom the disclosure was made;
 3. Whether the protected health information was actually acquired or viewed; and
 4. The extent to which the risk to protected health information has been mitigated.
4. When instructed to do so by the Iowa Medicaid HIPAA Liaison or the Iowa HHS Compliance and Administration Division, Bureau of Data Privacy and Strategy, (DPS), MCPs will mail DPS-approved breach notification letter(s) to the impacted member(s) or provider and send the Iowa Medicaid HIPAA Liaison a copy of the signed breach notification letter once mailed.
5. Initial Iowa HHS Incident Report – issue under investigation
 - a. In these instances, the MCP must submit the items in 3a. & 3b. above with the initial Iowa HHS Incident Report.
6. Unless otherwise agreed upon by the MCP and Iowa HHS, the MCP must submit an updated Iowa 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 Iowa HHS Incident Report.
7. CMS security incident report for dually eligible members
 - a. MCPs complete the CMS security incident report and submits to Iowa Medicaid HIPAA Liaison when an incident involves dually eligible members (when information involved originates from one of the following sources):
 - i. MMA Data File Exchange,
 - ii. State Buy-in File Exchange,
 - iii. TBQ File, and the
 - iv. previously disclosed Medicare A&B claims data for care coordination
8. Beginning calendar year 2024, MCP's shall submit breach notification to HHS-OCR Secretary, via OCR breach portal, according to § 164.408 Notification to the Secretary HIPAA breach notification requirements.

OCR Breach Portal: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf

- a. MCP shall provide a pdf copy of the submitted breach report to the Iowa Medicaid HIPAA Liaison.

The Iowa Medicaid Incident-HIPAA Liaison will take the following steps:

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

The DPS Bureau (Iowa HHS HIPAA Security Officer and HIPAA Privacy Officer and Legal Counsel) 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 conflicts with DPS's determination, notify the Iowa Medicaid Incident-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 Incident-HIPAA Liaison within three (3) business days.
5. Submit CMS security incident report to CMS when dually eligible members are affected.
6. Log the incident/breach and maintain copies of all documents.
7. Report the number of incidents and breaches to Iowa HHS management.

After DPS has completed the above steps, the Iowa Medicaid Incident-HIPAA Liaison will do the following:

1. Inform the MCP if DPS 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 DPS, when appropriate.
3. Schedule meetings between Iowa Medicaid, the MCP, and DPS, if the MCP has questions regarding their incidents/breaches, the need for breach notification, etc.
4. Send DPS a copy of the signed breach notification letter sent to the member or provider.

Related to this Policy Clarification:

- ▶ Effective date of this Policy Clarification: 12/01/2025
- ▶ Claims processing requirement:
 - ☐ Prospective
 - ☐ Retroactive
 - ☒ Not applicable

Attestation:

I hereby acknowledge receipt and understanding of this policy clarification, including all specified requirements and deadlines.

Name _____ Date _____

The department will monitor progress towards implementation and may impose remedies for failure to implement.

Sincerely,

Contract Manager
Managed Care Contract Manager