HEALTH CARE &
BENEFITS DIVISION

State of Montana Benefit Plan (State Plan) and Vendor Data Breach Notifications

Frequently Asked Questions

What happened?

Some State Plan members were impacted by recent data breaches involving vendors or subcontractors that provide services to the State Plan. These incidents did **not** involve state-owned computer systems or servers.

What steps is the State Plan taking to protect my information and prevent future breaches?

The Health Care & Benefits Division (HCBD) takes the protection of members' personal health information (PHI) very seriously.

Breaches involving State Plan data have occurred on the computer systems of contracted vendors or their subcontractors, not on state-owned servers. For example:

- **Conduent** is a subcontractor of Health Care Service Corporation, the parent company of BlueCross BlueShield of Montana (BSCSMT). BCBSMT is the State Plan's Medical Plan third party administrator. BCBSMT processes medical claims for the State Plan.
- **HCI Active** is a subcontractor of Allegiance Benefit Plan Management, Inc. Allegiance was the State Plan's Medical Benefit third party administrator from 2016 - 2022. Allegiance used to process medical claims for the State Plan.

HCBD requires all vendors that work with the State Plan (such as BCBSMT, Delta Dental, Navitus, and others) to:

- Comply with federal privacy and security laws
- Encrypt PHI both while stored and when transmitted
- Provide breach notifications to impacted individuals
- Offer credit monitoring and identity theft protection services when required

HCBD also requires its vendors to contractually hold their subcontractors to the same security and notification standards. HCBD actively works with vendors to ensure compliance with these requirements.

Why didn't the State Plan (HCBD) notify members directly?

Because these breaches occurred on vendor or subcontractor systems, HCBD did not have direct access to the detailed information needed to issue legally required notifications.

Under federal privacy laws, the organization that maintains or controls the affected data (and has the most accurate information about the incident) is responsible for notifying impacted individuals. That is why notices come directly from vendors or their subcontractors rather than from HCBD.

What support is being offered to impacted members?

HCBD requires vendors to provide credit monitoring and limited identity theft protection services to impacted individuals. The duration and type of assistance offered is based on the terms of the contact between HCBD and the vendor.

Details on how to enroll are included in the notification letters sent by the vendors.

Do I need to enroll in identity protection services for both incidents?

That decision is up to you. Each breach involved different vendors, and the notification letters outline steps you can take to protect yourself.

These steps may include:

- Monitoring your credit reports
- Placing fraud alerts with credit reporting agencies
- Requesting a credit or security freeze

HCBD encourages members to read each notice carefully and consider taking the recommended actions, particularly placing a credit or security freeze, which can offer strong protection against identity theft.

Where can I get more information?

Please refer to the notification letters you received from the vendors for detailed information about each incident and the services available to you.

If you have additional questions about your State Plan benefits, you may contact HCBD by calling (800) 287-8266, TTY (406) 444-1421, or emailing BenefitsQuestions@mt.gov.