Notification Requirements for Non-Compliance with CMS Regulations Focused on Data Loss, Misuse, or Breach

First Tier, Downstream, and Related Entities (FDRs) agree to comply with Medicare laws, regulations, and CMS guidelines. CMS regulations require that Medicare Advantage FDRs must retain relevant records and documentation related to their Medicare business for 10 years. FDRs also agree to report compliance concerns to CMS or the Plan. If an FDR knows of, or suspects, any non-compliance, they are required to report such non-compliance to the Plan Sponsor. Refer to your contracts to determine reporting requirements to carrier partners and uplines.

This bulletin is focused on the requirement to report the loss, misuse, breach, or failure to comply with record retention requirements to plan sponsors (carriers), uplines, and AmeriLife Compliance, if you are an AmeriLife Affiliate or an agent/agency in the AmeriLife hierarchy.

What is a data loss, misuse, or breach?

Data loss occurs when valuable or sensitive information is compromised due to theft, human error, virus, malware, or power failure. It may also occur due to

physical damage or mechanical failure. Examples of data loss might be accidental deletion of data, natural disaster, such as fire, flood, earthquake, or hurricane, malicious attack, such as hackers using ransomware or other malware to steal or destroy data, and system malfunction, such as technological errors or hardware failures that make data unreadable.

Misuse of data or breach means using information in a way that it is not intended or permitted, often violating privacy laws, company policies, or user agreements. Examples include sharing personal information without consent, improper sharing of PHI/PII data, manipulating data to mislead, or selling customer information without proper disclosure or consent.

A loss of data could be any type of loss – be it electronic or paper. Some examples include improper sharing of data with a third party or a data breach or data loss by a third party, such as a lost or stolen laptop, lost or deleted recordings of telephone calls/chain of enrollment calls, or mailing PHI/PII to an incorrect address.

When must an incident of data loss, misuse, or breach be reported?

Any time a required record is not maintained or compromised in any way, you must notify carriers, uplines, and AmeriLife Compliance. Data loss or misuse of data should be reported to carriers, uplines, and/or AmeriLife Compliance without reasonable delay once the data loss or breach/misuse of data is discovered, but no later than 48 hours from the date of discovery of the incident. Many states have reporting timeframes once a data loss or breach incident is discovered. If you are unsure if you have a data loss or misuse of data, contact HealthCompliance@AmeriLife.com for assistance.

How do I report an incident of data loss, misuse or breach?

Carrier contracts generally contain provisions for reporting any non-compliance. Please contact the carrier and report according to their specific reporting requirements. You should also contact your upline and Compliance@AmeriLife.com.

Examples of Data Loss, Misuse or Breach That Should Be Reported:

There are many types of data loss or breaches of data that must be reported such as:

- Lost or stolen computer/laptop/company cell phone (be sure to submit a police report regarding any stolen company device).
- Data was sent to someone who should not have received it, such as mailing a statement, bill, EOB, etc., that contained PHI/PII to the wrong person.
- Sending unencrypted data files or spreadsheets containing PHI/PII to the wrong person, email address, etc.
- Loss of data due to a natural disaster

What Information Needs to be Reported?

Data Loss or Breach/Misuse of Data reporting should include at a minimum:

- Date of incident
- Date of discovery of the incident
- Description of the incident, including how the data was compromised, how you discovered the incident, etc.
- Whether the incident involved electronic data, paper data, etc.
- The types of personal information that was compromised or lost (names, addresses, social security numbers, account/policy numbers, credit card numbers, bank account information, etc.)
- Affected individuals (names of agents, customers, potential customers, previous customers, etc.)
- The number of individuals impacted and their locations/states
- Names of carriers whose data was impacted by the incident
- Name, title, and contact information of person reporting the incident
- Name of agency reporting the incident
- Any steps taken to mitigate potential harm from the incident, including a detailed description of any steps taken.

- Whether you notified any agents, customers, carriers, etc., about the incident. including any relevant dates and what information was provided and to whom.
- Whether you have taken any steps or corrective action to prevent a new or ongoing incident, including a detailed description of any of these steps.