
October 4, 2018

Frequently Asked Question Regarding Web-broker Personally Identifiable Information (PII) Breach Incident Reporting

The following question and answer provides clarification about the Centers for Medicare & Medicaid Services (CMS) requirements for web-broker PII incident or breach reporting.

1. What actions must web-brokers take if a suspected or confirmed incident or breach of Personally Identifiable Information (PII) occurs?

Per the standards set forth in the *Agreement Between Web-Based Entity and the Centers for Medicare & Medicaid Services for the Federally-Facilitated Exchange and the State-Based Exchange on the Federal Platform Individual Market* (Agreement), web-brokers agree to report any suspected or confirmed Incident or Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within one hour of discovery of the Incident or Breach.

In the event of an Incident or Breach, web-brokers must permit CMS to gather all information necessary to conduct all Incident response activities deemed necessary by CMS. If web-brokers fail to report an Incident or Breach in compliance with this provision, the web-broker may be subject to the Termination provision (Section IV) of the Agreement. Termination pursuant to Section IV may also result where an Incident or Breach is found to have resulted from a web-broker's failure to comply with the terms of the Agreement.

Per Section 6 in Appendix A of the Non-Exchange Entity Privacy and Security Standards and Implementation Specifications section within the Agreement, web-brokers should also adopt and implement the standards and implementation specifications in the Agreement in a manner that ensures appropriate monitoring and other means and methods to identify and report Incidents and/or Breaches.