



December 14, 2018

Reminders to Qualified Health Plan Issuers: CMS QHP Agreement Requirements for Personally Identifiable Information Breach and Security Incident Reporting

The safety and security of consumer information is our number one priority. The following question and answer highlight key information regarding requirements for Qualified Health Plan Issuers (QHPI) Personally Identifiable Information (PII) Incident or Breach reporting. These requirements are included in the Agreement Between Qualified Health Plan (QHP) and the Centers for Medicare & Medicaid Services that QHPI sign before they participate in the Exchange by displaying plans to consumers.

1. What actions must a QHPI take if a suspected or confirmed Incident or Breach of PII occurs?

Per the *Agreement Between Qualified Health Plan (QHP) and the Centers for Medicare & Medicaid Services* (Agreement), QHPI agrees to report any suspected or confirmed Breaches 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 24 hours of discovery of a Breach. Suspected or confirmed Incidents must be reported to the CMS IT Service Desk by the same means as Breaches within 72 hours of discovery of the Incident. In the event of an Incident or Breach, QHPIs must permit CMS to gather all information necessary to conduct all Incident or Breach response activities deemed necessary by CMS.

2. What happens if a QHPI fails to report a suspected or confirmed Incident or Breach involving PII?

If QHPI fails to report an Incident or Breach in compliance with this provision, the issuer may be subject to the Termination provision (Section V) of the Agreement. Termination pursuant to Section V may also result where an Incident or Breach is found to have resulted from QHPI's failure to comply with the terms of the Agreement. Nothing in the Agreement should be construed to limit the ability of the Department of Health & Human Services (HHS) to temporarily suspend the ability of a QHPI to connect to HHS systems due to suspected or confirmed security risks and Incidents or Breaches.