



# CMS Office of the Administrator Incident and Breach Response Playbook

# Welcome to Our Incident

You have been just informed that there has been a potential incident within one of the CMS programs. This playbook will walk you through key steps and processes you need to be aware of. While the Office of Information Technology (OIT), Information Security and Privacy Group (ISPG) Incident Management (IMT) and the Privacy Breach Response teams will lead the incident and breach response activities, you have a very integral part to play in the response activities.

## Breach Confirmation

Once there has been confirmation of a breach of PII or PHI, the Incident Management team will begin scheduling stand-ups with the Breach Response Team (senior leadership team). This includes the COO (this could also be the Deputy COO). The COO is directly responsible for keeping the Administrator informed throughout the breach response activities and is the representative for OA on the Breach Response Team. As part of the breach confirmation process, IMT will populate a “Breach at a Glance” information page for the COO to have the most up-to-date information regarding the breach for briefing the Administrator as needed.

Below is a sample “Breach at a Glance” :



### Breach Response Team Activities

As a member of the Breach Response Team, the COO will attend standup meetings. The cadence of these meetings will be determined by size and complexity of the breach. Updates are sent from the Breach Analysis Team, at times with action items for the Breach Response Team. The breach analysis, beneficiary notification letter, media notification, and Office for Civil Rights notification are presented to the Breach Response Team for review, prior to review by our Office of General Council, CMS Division points of contact.

<b>What:</b>	<b>Breach of Claims data</b>
<b>When:</b>	12/5/2023
<b>CMS System:</b>	No. Contactors corporate system
<b>Name of System:</b>	N/A
<b>Center/Office:</b>	Center for Medicare
<b>Contractor:</b>	ZAP Federal
<b>Number of Records:</b>	9,888,887
<b>Major Incident:</b>	Yes
<b>Notification Deadlines:</b>	Initial Congressional: 12/11/2023 30 Day Congressional: 1/3/2024 HIPPA Notifications: 2/2/2024
<b>High-level Summary:</b>	Claims data was being stored on a local server at ZAP Federal. The claims data was downloaded by an individual onto an external hard drive. Law enforcement is involved but they were unable to locate the hard drive and the individual is uncooperative. There is a reasonable expectation that the information has been released to addition individuals with bad intent.

If CMS or HHS has declared a Major Incident under FISMA, the COO will also review any Congressional Notifications prior to being sent to HHS and may have to participate in any Congressional Briefings requested. Participation in these briefings would be in support of the Administrator/Principal Deputy Administrator and may also include Office of Information Technology leadership.

## Ad Hoc Breach Response Activities

At times, during breach response activities, there are ad hoc meetings that may be coordinated. These meetings are traditionally focused on contractor issues that come up during breach response. The COO may need to step in these meetings, to assist the breach analysis team gather the needed artifacts from the contractor.

Other meetings that may arise during breach response are with HHS, OIG, DOJ or other Federal partners. COO will be briefed on the issues that are being addressed during the ad hoc meeting at the stand-up just prior to the meeting occurring. Updated documentation and briefing notes will also be provided for the meeting.

## Responsibilities

### CMS Administrator

The responsibilities of the CMS Administrator include, but are not limited to, the following:

- a. Provide a representative to the CMS Breach Response Team in the event of a major incident (the COO, Deputy COO or both)
- a. Act as the Notifying Official;
  - i. With the approval of the HHS Breach Response Team, notify individuals potentially affected by a particular breach of services offered to mitigate the risk of harm (to be completed by SOP and Breach Analysis Team on behalf of the Notifying Official).
  - ii. When a breach affects a vulnerable population, consider the need to provide a different type of notification to that population or provide a notification that would otherwise not be necessary (to be completed by the Breach Response Team on behalf of the Notifying Official.)
- b. Obtain the approval of the HHS Breach Response Team prior to designating a senior official as a Notifying Official.

## Reporting Triggers

Trigger	Requirement	Responsible Party
---------	-------------	-------------------

All Incidents	Notify HHS, notify US-CERT (United States Computer Emergency Response Team)	HHS is automatically notified by the CMS incident ticketing system; HHS handles reporting to US-CERT
All Suspected or Confirmed Breaches	Conduct Risk Assessment	If the breach is not in a predefined low-risk category, the CMS Breach Analysis Team must convene.
Greater than 500 individuals within same jurisdiction are affected by a breach	Notify media in affected jurisdiction within 60 days, at the same time as individual notification	Office of Communication as part of the Breach Response Team
Substitute Notification	More than 10 items of returned mail	Office of Communication as part of the Breach Response Team
Greater than 100,000 individuals are affected by the breach (Major Incident)	Notify Congress within 7 days, Follow up notification in 30 days Possible in-person Congressional Briefings.	Office of Legislation as part of the Breach Response Team

## Reporting Timelines

### Timeline: HIPAA



### Timeline: FISMA Major Incident and HIPAA

