

CMS INFORMATION SYSTEM SECURITY OFFICER

INCIDENT & BREACH RESPONSE PLAYBOOK

OIT/ISPG
CISO@CMS.HHS.GOV



Introduction

This handbook gives practical guidance to Information System Security Officers (ISSOs) at CMS when performing their necessary tasks. It helps new ISSOs get started and explains the responsibilities, resources, and organizational relationships needed for an ISSO to be successful.

This guide is for CMS (Federal) ISSOs, Contractor ISSOs, and contract security support individuals. Business owners and their staff may also find parts of this handbook useful, particularly when appointing new ISSOs or gaining a better understanding of ISSO tasks. The ISSO role is critical to the safe and authorized use of sensitive information in support of CMS' commitment to improving healthcare for millions of americans.

As an ISSO, every CMS system must formally designate an ISSO who serves as the primary point of contact responsible for the system's security and privacy along with be a part of the Breach Analysis Team (BAT) and the Breach Response Team.

ISSOs at CMS are responsible for overseeing the security and privacy posture of the system(s) entrusted to their care, coordinating all information system risk management and information privacy activities, and acting as the Business Owner's "go-to person" for security questions and needs. Together, the ISSOs make up a supportive community working to ensure the success of the cybersecurity program at CMS.

Welcome to Your Incident

You have been just informed that there has been a potential incident within one of your 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 Breach Response teams will lead the incident and breach response activities, you have a very integral part to play in the response activities.

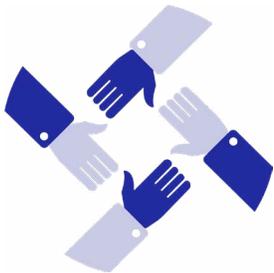
STEP 1



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 Analysis Team (staff level team) and the Breach Response Team (senior leadership team). The Business Owner of the Affected Program or their designee is expected to participate as a member of the Breach Response Team. Once you receive the notification of the confirmed breach, if you would like to designate an alternate to attend the breach response team calls, please respond to the notification email with the name of your designee(s) and provide a copy of this playbook to them.

STEP 2

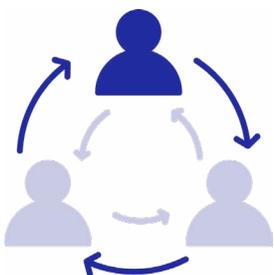


Breach Response Team Activities

As a member of the Breach Response Team, the business owner 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.

If CMS or HHS has declared a Major Incident under FISMA, the Business Owner 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.

STEP 3



After Action

The Business Owner and other stakeholders from the Affected Program office are expected to participate in any after action activities. These activities help the agency refine incident and breach response activities, prior to the next reported breach.

Who is on the BAT?

The Breach Analysis Team (BAT) consists of breach response stakeholders in leadership positions and security and privacy subject matter experts for the affected system.

This may include:

- Representatives from the Incident Management Team (IMT) within the CMS Cybersecurity Integration Center (CCIC)
- Representatives from ISPG (which may include the DCTSO Incident Commander and Senior Official for Privacy)
- Business and/or System Owner of the affected system

Other people, as needed:

- Information System Security Officer (ISSO)
- System Maintainer
- Contracting Officer Representative (COR) – if the affected system is a contractor system
- CPI point of contact

BAT Responsibilities and Steps

Once convened, the BAT is responsible for the following:

Conduct a Risk Assessment, reviewing:

- ✓ How sensitive is the PII?
- ✓ How likely is the PII to be accessed and used?
- ✓ What kind of breach?
- ✓ Who is involved?
- ✓ What is CMS' ability to mitigate risk?

Once completed, the BAT is to document the results of the above assessment on the Risk Assessment for Breach Notification worksheet, and submit the completed form to the CMS Senior Official for Privacy: privacy@cms.hhs.gov.

If the above Risk Assessment indicates that there is a low probability that the PII has been compromised, inform the Incident Management Team of the Risk Assessment so they can coordinate with the CMS Computer Security Incident Response Team (CSIRT) to update and close the applicable ticket.



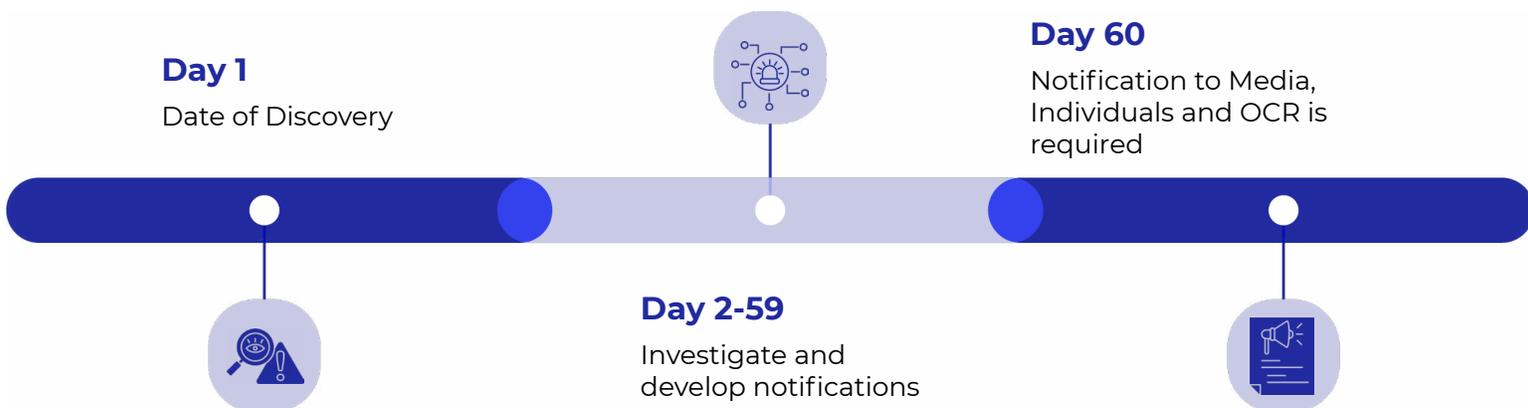
For additional processes and procedures, determinations of severity of breaches, and notifications procedures, please review the [CMS Breach Analysis Team \(BAT\) Handbook](#) and the [CMS Breach Response Handbook](#).

Reporting Triggers

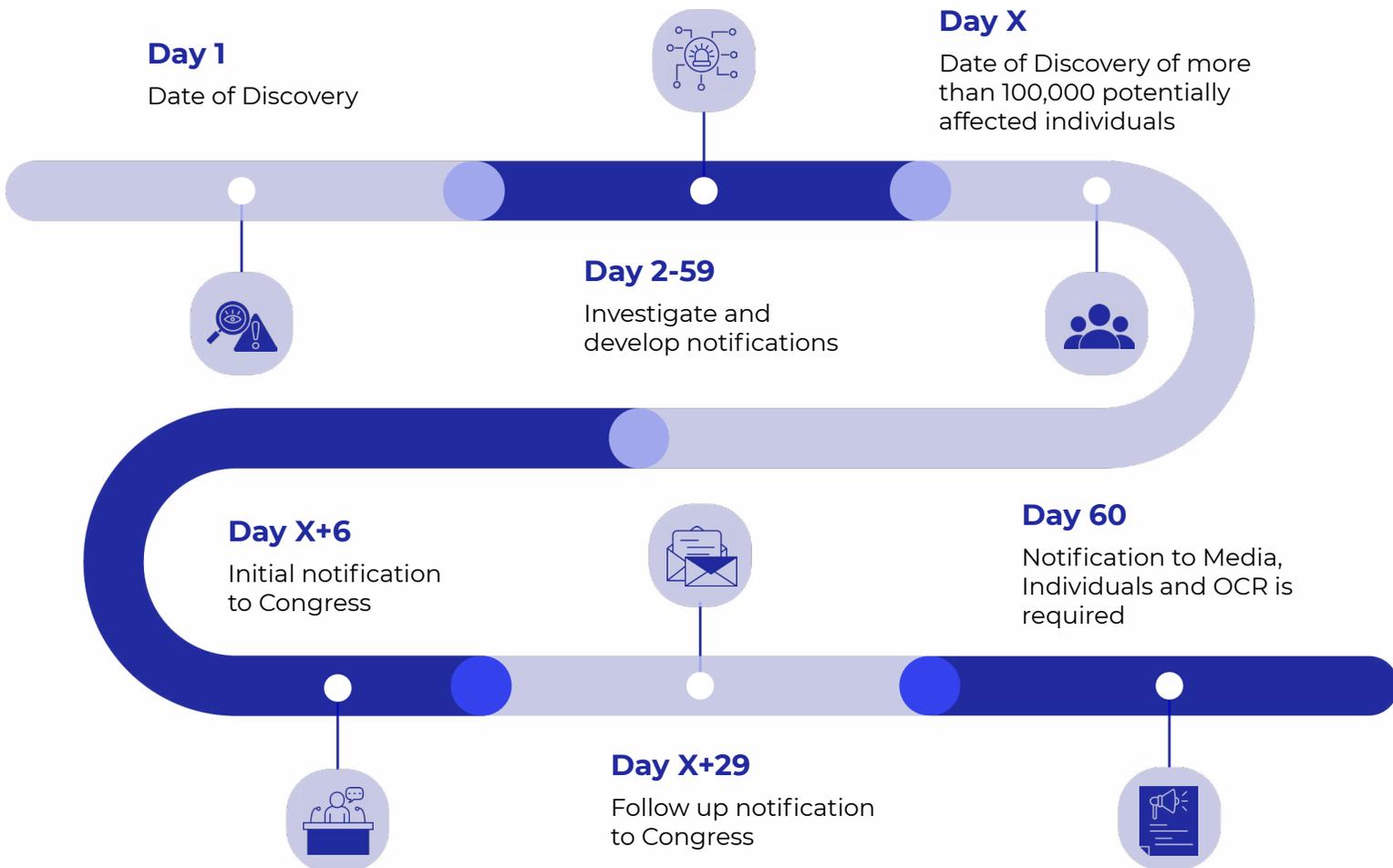
Trigger	Requirement	Responsible Party
All Incidents	Notify HHS, notify US-CERT (United States Computer Emergency Response Team)	HHS is automatically notified by the CMS incident ticketing system; HHS handles reporting to US-CERT
All Suspected or Confirmed Breaches	Conduct Risk Assessment	If the breach is not in a predefined low-risk category, the CMS Breach Analysis Team must convene.
Breach Analysis	<ul style="list-style-type: none"> • HHS Privacy Incident Response Team (PIRT) review • PIRT reviews the Breach Risk Assessment final individual notification draft and recommended mitigations 	Breach Analysis Team
Notification of Individuals	<p>Individual notification needs to be sent to potentially affected individuals within 60 days following the discovery of a breach and must include:</p> <ul style="list-style-type: none"> • a brief description of the breach, • a description of the types of information that were involved in the breach, • the steps affected individuals should take to protect themselves from potential harm, • a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, • as well as contact information for the covered entity (or business associate, as applicable). 	Breach Analysis Team after review by the Breach Response Team and the HHS Breach Response Team/HHS Privacy Incident Response Team
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
Notice to the Secretary (Office for Civil Rights (OCR) portal)	Report submitted on OCR portal with all details of the incident and remediation/mitigation efforts within 60 days, at the same time as individual notification	Senior Official for Privacy
Breach Indicates Illegal Activity	Contact Law Enforcement via HHS oversight body	Contact HHS Office of Inspector General (OIG) Computer Crimes Unit (CCU)
Breach Affects FTI	Notify IRS and U.S. Treasury Inspector General for Tax Administration (TIGTA)	Contact CMS-IRS Liaison
Greater than 100,000 Individuals are Affected by the Breach (Major Incident)	<ul style="list-style-type: none"> • Notify Congress within 7 days • Follow up notification in 30 days • Possible in-person Congressional Briefings. 	Contact Office of Legislation (OL)

Reporting Timelines

Timeline: HIPAA



Timeline: ISMA Major Incident & HIPAA



Responsibilities

ISSO from the Affected Program Office

The Affected Program Office is the organization where the breach occurred, or if the breach occurred at a non-CMS entity managing federal information or a federal information system on behalf of CMS, the organization with programmatic oversight of that entity.

The responsibilities of the Affected Program Office include, but are not limited to, the following:

Serve on the Breach Analysis Team (staff level).



In coordination with the CMS SOP and the CMS Breach Analysis Team, assess whether the data involved is PII/PHI.



Confirm whether the data involved in a potential breach is federal data.



For all breaches involving contractors or subcontractors, confirm the Contracting Officer is aware of the breach.



In coordination with the CMS SOP, identify all the applicable privacy compliance documentation, such as system of records notices (SORNs), privacy impact assessments (PIAs), and privacy notices on information collection instruments related to the breach.



In coordination with the CMS Breach Analysis Team, seek additional information, as necessary, to reconcile or eliminate duplicate records, identify potentially affected individuals, or obtain contact information to provide notification.



In coordination with the CMS Breach Analysis Team, develop a robust response plan and a draft notification letter(s).

