U.S. Department of Health & Human Services

Office of Inspector General

States Follow a Common Framework in Responding to Breaches of Medicaid Data

OEI-09-16-00210
October 2018

oig.hhs.gov

Suzanne Murrin
Deputy Inspector General
for Evaluation and
Inspections

Report in Brief
October 2018
OEI-09-16-00210

U.S. Department of Health & Human Services
Office of Inspector General

States Follow a Common Framework in Responding to Breaches of Medicaid Data

Key Takeaway
Most Medicaid data breaches in 2016 affected few beneficiaries, and many breaches resulted from misdirected communications. All States have established processes to respond to breaches, including notifying affected individuals. However, although CMS guidance advises States to notify CMS of breaches, most States do not routinely do so.

What OIG Found

In 2016, State Medicaid agencies and their contractors identified 1,260 data breaches. The characteristics of these breaches varied widely, but they typically affected few beneficiaries; often resulted from misdirected communications, such as letters and faxes; and exposed beneficiaries' names and Medicaid or other identification numbers. Breaches that resulted from hacking or other IT incidents were rare.

Most States' breach-response plans follow a common framework: (1) learning about incidents; (2) assessing incidents and determining how to respond; (3) taking steps to protect those affected; and (4) correcting vulnerabilities. However, the specific actions that States take vary depending on the circumstances of each breach and on any applicable State laws and requirements. These State actions address the potential harm that breaches can pose to Medicaid beneficiaries and programs.

Almost all States reported learning about breaches from contractors and their employees. Many States also have received breach reports from beneficiaries and/or their family members and medical providers. For some breaches, State Medicaid agencies and their contractors conducted forensic analyses of their information systems and worked with law enforcement agencies to further investigate the breaches. States reported that, in their efforts to protect Medicaid beneficiaries, they notified people who were affected by breaches and typically offered them services for credit monitoring and for protection against identity theft. In some cases, States reported issuing beneficiaries new Medicaid identification numbers when the old numbers were compromised. States described corrective actions, such as retraining employees; modifying policies and procedures; and restricting access to protected health information to address vulnerabilities that allowed the breaches to occur.

States' breach-response processes also address the requirements under the Breach Notification Rule—part of the Health Insurance Portability and Accountability Act (HIPAA)—for States to notify affected individuals and the Department of Health and Human Services' Office for Civil Rights. In 2006, the Centers for Medicare & Medicaid Services (CMS) issued guidance advising States to inform CMS of breaches of Medicaid data. Some States stated that they report breaches to CMS in certain circumstances; however, most States said that they do not routinely do so.

What OIG Recommends and Agency Response

We recommend that CMS reissue guidance to States about reporting Medicaid breaches to CMS. Collecting information on a national scale regarding Medicaid data breaches could help CMS identify breach trends and promote effective State responses. CMS concurred with our recommendation.

Full report can be found at oig.hhs.gov/oei/reports/oei-09-16-00210.asp

Why OIG Did This Review

State Medicaid agencies and their contractors maintain and process health information for millions of beneficiaries. Prior OIG reviews have identified vulnerabilities in States' information systems and controls—vulnerabilities that could have resulted in unauthorized disclosure of protected health information (PHI). States must be prepared to respond to breaches to limit potential harm, such as identity theft and fraudulent billing.

How OIG Did This Review

We collected information about all breaches that Medicaid agencies and their contractors reported experiencing in 2016. We also surveyed 50 States and the District of Columbia to learn more about their processes for responding to breaches of PHI. Lastly, we interviewed and reviewed documents from officials in nine States to learn more about how each State responded to a specific breach that we selected and about their breach-response processes more generally. For each of these nine breaches, we examined how the State learned about the incident; how it determined whether the incident constituted a breach under HIPAA; how the State and others investigated the breach; and what actions the State took to protect its beneficiaries and programs and to correct vulnerabilities.

TABLE OF CONTENTS

BACKGROUND

Objectives

1. To determine characteristics of breaches of protected health information that State Medicaid agencies and their contractors experienced in 2016.
2. To examine how State Medicaid agencies respond to breaches that they or their contractors experience.

Breaches of unsecured protected health information (PHI) can create vulnerabilities for State Medicaid programs and their beneficiaries. Such breaches can expose beneficiaries to identity theft or other types of harm and leave Medicaid programs susceptible to fraud. State Medicaid agencies must be prepared to respond to breaches and limit any associated harm to beneficiaries, providers, and the program.

Medicaid agencies and their contractors maintain and process health information for millions of individuals. (For the purposes of this report, a "contractor" is an entity that may have a business-associate relationship with a State Medicaid agency or may be participating in an organized health care arrangement with a State Medicaid agency.) As of July 2018, 67 million beneficiaries—about 20 percent of the U.S. population—received their health care through Medicaid.[1] State Medicaid databases contain PHI on beneficiaries, including Medicaid identification numbers, medical diagnoses, treatments, and providers. These databases also contain demographic and financial information that States use to assess an applicant's eligibility for Medicaid. In addition to being present within State databases, Medicaid beneficiary information also may be maintained, processed, and transmitted by

What is a breach?

The Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule defines a breach as the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule that compromises the privacy or security of that information. The HIPAA Breach Notification Rule applies to breaches of unsecured PHI that has not been rendered unusable, unreadable, or indecipherable by encryption, destruction, or other methods.

What is protected health information?

Protected health information refers to information about an individual's physical or mental health or condition, the provision of health care, or payment for the provision of health care that includes personal identifiers, such as names or medical record numbers.

Source: 45 CFR pt. 164, subpt. D

[1] Kaiser Family Foundation. *July 2018 Medicaid & CHIP Enrollment Data Highlights*. Accessed at https://www.medicaid.gov/medicaid/program-information/medicaid-and-chip-enrollment-data/report-highlights/index.html on October 2, 2018. This information does not include the territories.

organizations such as managed care organizations (MCOs) and fiscal agents with which the State Medicaid agencies contract.

Reporting of Breaches to Federal Authorities

The HIPAA Breach Notification Rule[2] spells out notification and other actions that all covered entities—including Medicaid agencies and their contractors—must take in response to a breach of PHI. The rule generally requires that in response to a breach of PHI, covered entities must notify affected individuals, the Department of Health and Human Services' Office for Civil Rights (OCR), and (in certain instances) the media.[3] Notifications are intended to alert affected individuals about a breach and to provide information that they can use to limit its impact.

As the Federal agency that administers the Medicaid program, CMS issued guidance in 2006 specifying that State Medicaid agencies "should immediately report a breach, whether discovered by [an agency's] own staff or reported by a contractor" to CMS.[4] CMS reiterated in the guidance that State Medicaid agencies must abide by all Federal and State laws related to protecting PHI, and that CMS considered breaches of Medicaid data to be serious matters that could result in CMS's suspending or denying a Medicaid agency's Federal financial participation for the agency's information systems.[5]

Related Work

This evaluation builds on a body of work by the Office of Inspector General (OIG) on protecting individuals from vulnerabilities related to the security of health information. Prior reports have described how OIG found high-risk security vulnerabilities in State Medicaid agencies' information systems and inadequate controls that could have resulted in unauthorized disclosure of PHI.[6, 7] The audits found that data was at risk of unauthorized disclosure due to vulnerabilities related to access controls and lack of formal policies. OIG recommended that State Medicaid agencies address the specific vulnerabilities that it identified and make information system security a higher priority.

[2] 45 CFR §§ 164.400-414. The Breach Notification Rule implements provisions of the Health Information Technology for Economic and Clinical Health Act, which was passed as part of the American Recovery and Reinvestment Act of 2009.

[3] 45 CFR §§ 164.400-414. For breaches that affect 500 or more people, Medicaid agencies and other covered entities must report the breach to the media, as well as to OCR and affected individuals. Generally, these notifications must be completed within 60 days following the discovery of a breach. For breaches that affect fewer than 500 individuals, covered entities can notify OCR in their annual reporting.

[4] CMS, *State Medicaid Director Letter #06-022*. Accessed at https://downloads.cms.gov/cmsgov/archived-downloads/SMDL/downloads/SMD092006.pdf on October 2, 2018.

[5] Ibid.

[6] OIG, *Inadequate Security Management Practices Left the Utah Department of Health Sensitive Medicaid Data at Risk of Unauthorized Disclosure*, A-07-15-00455, January 2016.

[7] OIG, *High-Risk Security Vulnerabilities Identified During Reviews of Information Technology General Controls at State Medicaid Agencies*, A-07-14-00433, March 2014.

Methodology

Data Collection and Analysis

We collected information about breaches that Medicaid agencies and their contractors experienced in 2016. We also surveyed Medicaid agencies, and we conducted interviews with State officials regarding nine selected breaches.

Medicaid Breaches in 2016. We requested that Medicaid agencies submit to us information about all breaches that they and their contractors experienced in 2016.[8] We requested breach information from Medicaid agencies in all 50 States and the District of Columbia (States) and analyzed it to determine characteristics of the breaches that they and their contractors experienced in 2016. These characteristics include the number of beneficiaries and other individuals affected by each breach; the type of information disclosed in breaches; and how breaches occurred.

State Processes for Responding to Breaches. We surveyed all States about their processes for responding to Medicaid breaches. We analyzed the results to identify processes that States have to do the following: (1) collect information about breaches, (2) determine how to respond to breaches, (3) protect those affected, and (4) address the vulnerabilities that allowed the breaches to occur.

We conducted in-depth reviews of nine Medicaid breaches (each in a different State). We selected these breaches using States' responses to the survey and information about the breaches that they experienced. To examine how States responded to different types of breach scenarios, we selected breaches on the basis of the following characteristics: the number of individuals affected, the type of PHI disclosed (e.g., whether health information was included), and how the breach occurred. The nine breaches varied in terms of the number of people affected (from 1 to about 370,000); the types and amounts of PHI disclosed (some disclosed extensive health and financial information, whereas others disclosed only limited personal identifiers); and the cause of the breach (ranging from misdirected email to IT hacking). For each of these breaches, we interviewed the State officials responsible for responding to the breach, and gathered documentation related to the State's response to the breach.

Limitations

Our analysis of breaches from 2016 relied on data we received from State officials. Therefore, it is possible that States over-reported or under-reported to OIG the number of applicable Federal breaches that their Medicaid agencies or their Medicaid contractors experienced in 2016. For example, some contractors may not be contractually required to notify their respective States of breaches and, therefore, we may not have received all breach reports from those States.

[8] We focused our review on breaches experienced directly by Medicaid agencies and their contractors. Our analysis does not include other breaches that may have affected Medicaid beneficiaries, such as those that occurred in hospitals or provider offices.

We did not verify whether States reported to us all Federal breaches that they identified. We also did not verify whether the breaches that States reported to us constituted breaches as defined by HIPAA.

Our analysis of State processes for responding to breaches also relied on information that State officials provided via surveys. For the breaches that we examined in-depth, we interviewed State officials and reviewed documents related to their respective States' responses to breaches; however, we did not independently verify that their States carried out the activities that they reported.

Standards

This study was conducted in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

FINDINGS

Most Medicaid breaches in 2016 disclosed information about a single individual, and often resulted from misdirected letters or faxes; large breaches from hacking were rare

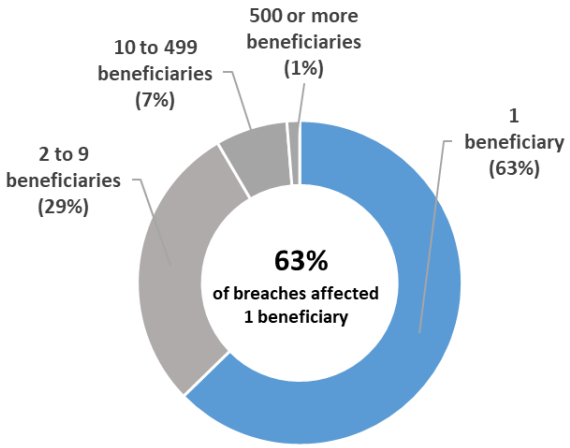
Medicaid agencies and their contractors in 36 States reported that they experienced a total of 1,260 breaches in 2016.[9] The other 15 States reported that they or their contractors did not experience a breach that year. About two-thirds of the breaches were experienced by Medicaid contractors; the remaining third were experienced by Medicaid agencies. These breaches varied widely in three key characteristics: (1) the number of people affected by the breach, (2) the kind of PHI disclosed, and (3) how the breach occurred.

Most Medicaid breaches affected few beneficiaries

As shown in Exhibit 1, nearly two-thirds of breaches disclosed data about a single person and almost 30 percent involved disclosures that affected between 2 and 9 beneficiaries. States reported approximately 515,000 beneficiaries and other individuals (hereinafter referred to as beneficiaries) as having been affected by the breaches in 2016.[10]

A small percentage (1 percent) of breaches disclosed data that affected 500 or more beneficiaries. For example, one State reported a breach affecting approximately 370,000 beneficiaries in 2016. The State said that the breach was caused by an individual who hacked the computer server of an MCO's business associate and had access to names, dates of birth, diagnosis information, and Social Security numbers (SSNs). The State concluded that there was no evidence that the individual intended to use the information fraudulently. This breach represents approximately 72 percent of the total number of individuals affected by Medicaid breaches reported by all States in 2016; it was by far the largest breach reported. See Appendix B, Breach Case 3 for more information about this breach.

Exhibit 1: Most Medicaid breaches in 2016 affected few beneficiaries



Source: OIG analysis of 2016 breaches experienced by State Medicaid agencies and contractors. The exhibit excludes six breaches for which the respective States did not provide enough information for OIG to categorize.

Some small 2016 breaches had the potential to negatively impact beneficiaries

- A beneficiary's drug test results were disclosed to an ex-girlfriend.
- A beneficiary's address was disclosed to an ex-boyfriend who had previously stalked and assaulted the beneficiary.
- A beneficiary's participation in a substance abuse treatment program was disclosed to the beneficiary's coworkers.

Source: OIG analysis of 2016 breaches.

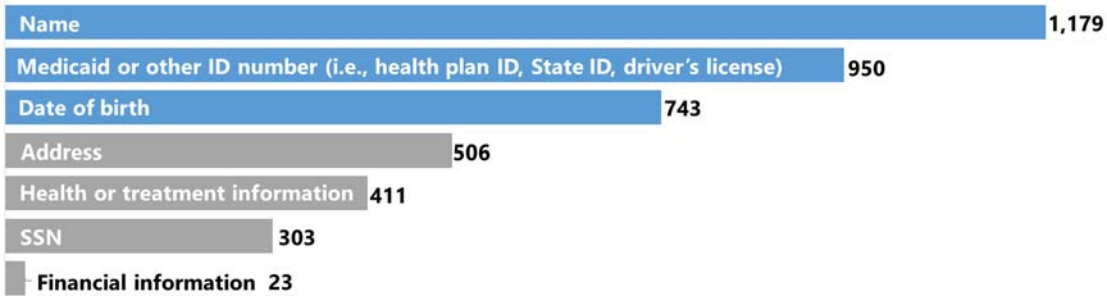
[9] We defined "Medicaid contractor" as any entity that (1) has access to Medicaid-related PHI and (2) has entered into an agreement with a State Medicaid agency to perform Medicaid-related functions. Examples include claims processors, managed care organizations, pharmacy benefits managers, or mailing companies.

[10] Some breaches may have affected individuals who were not Medicaid beneficiaries, such as beneficiaries' family members and people who are not Medicaid beneficiaries but are enrolled in managed care plans that also serve Medicaid beneficiaries.

Most breaches involved beneficiary names and other identifiers.

Almost all breaches in 2016 disclosed at least the names of Medicaid beneficiaries. As shown in Exhibit 2, many breaches also disclosed Medicaid/health plan numbers, driver's license numbers, and/or dates of birth. Less commonly disclosed types of information were beneficiary addresses, health information, SSNs, and financial information (e.g., bank/credit card information).

Exhibit 2: Medicaid breaches in 2016 most often involved beneficiary names, identification numbers, and/or dates of birth

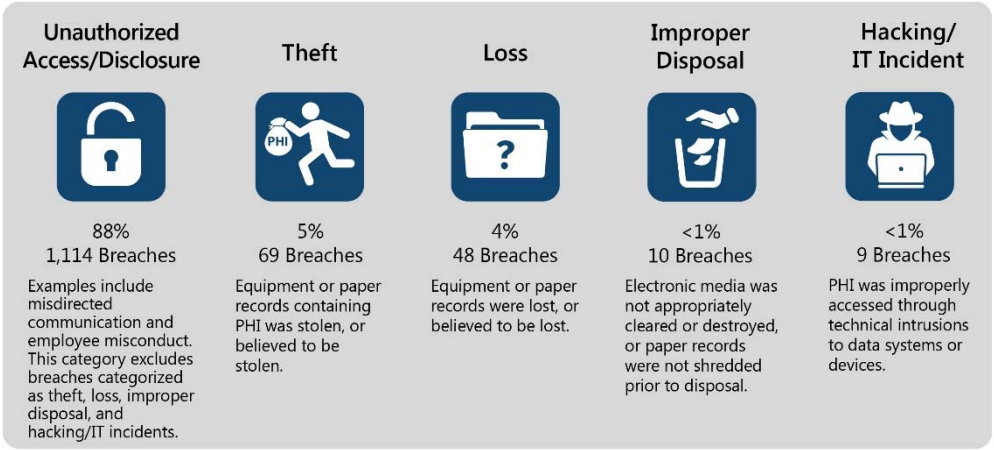


Source: OIG analysis of breaches that Medicaid agencies and contractors experienced in 2016.

Most breaches were due to unauthorized access or disclosure

As shown in Exhibit 3, most breaches that occurred in 2016 resulted from unauthorized access or disclosure of PHI—for example, mail being misdirected or beneficiary PHI being accessed by employees who lacked the authority to do so. Often in these cases, communications (e.g., letters, faxes, or emails) that contained beneficiaries' PHI were sent to the wrong place, such as to the wrong beneficiary or physician office. Other breaches in this category occurred when employees or family members improperly accessed or shared PHI without a legitimate business or medical need.

Exhibit 3: Few Medicaid breaches were a result of hacking/IT incidents in 2016



Source: OIG analysis of breaches that Medicaid agencies and contractors experienced in 2016. The breach categories are based on those that OCR provides on its online portal for covered entities to report breaches. The exhibit excludes 10 breaches for which the State did not provide enough information for OIG to categorize the breach.

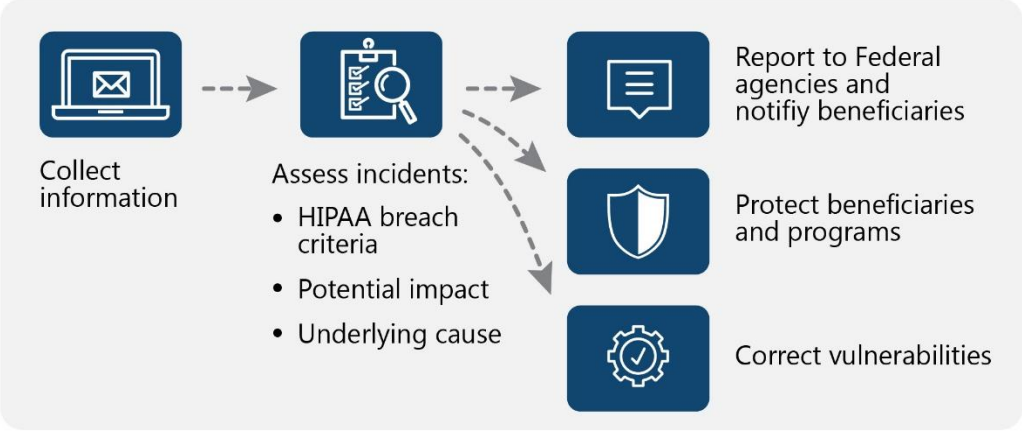
Other breaches resulted from theft, loss, and improper disposal of PHI. Breaches resulted from laptops or documents being stolen from cars or during burglaries of pharmacies and medical offices. States also reported that some breaches resulted from losing or misplacing items—specifically, a file cabinet, a daily planner, and a portable storage device. Additionally, States reported that breaches resulted from improper disposal, such as when Medicaid employees or their contractors improperly discarded records in unsecured recycling bins.

Few reported breaches were due to hacking incidents. For the ones that were, States reported that the breaches resulted from ransomware and phishing attacks, and other attempts to access sensitive data or systems without authority. The targets of the hacking incidents were MCOs and other health plans as well as their subcontractors, such as data processing companies and laboratory facilities. In addition to the above-described hacking incident that affected 370,000 individuals, there were 8 other hacking incidents that affected another 5,500 individuals.

States have processes for collecting information about breaches and suspected breaches and determining whether to report these incidents to Federal agencies

All 51 States have developed processes for learning about and responding to Medicaid breaches. As shown in Exhibit 4, these processes generally start with collecting information about breaches and potential breaches and assessing them to determine how to respond. Although most States' responses to breaches follow a common framework, the specific actions they take vary depending on the circumstances of each breach, and any applicable State laws and requirements.

Exhibit 4: States' processes for responding to breaches follow a common framework. These activities can occur either sequentially or concurrently



Source: OIG synthesis of information collected through State surveys, interviews, and documents.

States have established reporting requirements and proactive practices to help ensure that they learn about breaches and suspected breaches

States have processes that require breaches to be reported directly to the agency or individual in charge of the State's breach response. Further, States often seek information about all privacy and security incidents involving Medicaid data, regardless of whether the incidents have been confirmed as constituting breaches under HIPAA. Although most States have established requirements for all of their Medicaid contractors to report breaches, several States specified that these requirements apply only to certain contractors, such as those that have access to PHI.

States reported collecting—in incident reports—detailed information about breaches and suspected breaches. States typically require employees and contractors that report breaches and suspected breaches to provide information about the cause, nature, and scope of any unauthorized disclosure. For example, they request information about:

- the nature of each incident, including how it occurred and/or the type of media that contained the PHI;
- the type of PHI or other information that was disclosed;
- the number of individuals affected;
- the date of the incident and its discovery; and
- any steps taken to limit the exposure of PHI.

Some States told us that when they experienced a breach, they required contractors and/or employees to report additional information, such as actions that they or others took to respond to the incident. For example, they requested information about any steps taken to investigate the incident, to correct vulnerabilities, or to complete breach notifications. Almost all States reported that they have learned about breaches from contractors and their employees. Many States also have received breach reports from beneficiaries and/or their family members, and from medical providers and/or healthcare facilities. For the nine breaches that we examined more closely, States received incident reports through online reporting systems, emails, phone calls, and in-person conversations with contractor staff and States' own employees.

States also have proactive methods to identify breaches. States reported implementing proactive practices to identify breaches and suspected breaches. For example, most States reported conducting system audits and surveillance to identify instances of unauthorized access to data systems. Additionally, several States described other activities, such as regularly training staff on how to identify and report incidents; scanning outbound employee emails for PHI; and providing outlets for the public to report privacy and security concerns.

States' breach responses can involve coordination across multiple State agencies

Although most States designate a lead agency for responding to breaches and suspected breaches, their responses can involve multiple agencies. Most States reported that privacy officials positioned within either the Medicaid agency or an umbrella health and human services agency take the lead in collecting information about breaches and responding to them. However, almost half of States noted that their responses to breaches can involve coordination across multiple State agencies. For example, one State reported that its Medicaid privacy officer typically takes the lead, but that its Chief Information Officer and Information Security Officer would be involved in investigating or responding to cybersecurity incidents. In other States, laws or policies require the lead breach-response agency to report information about breaches that meet certain criteria (e.g., breaches that affect more than 500 people, involve personal identifiers, or result from fraud) to other entities, such as the Governor's Office or State Attorney General.

States and their contractors have processes for assessing privacy and security incidents to determine whether they must be reported to OCR

States use information from incident reports and any subsequent investigations to determine or confirm whether privacy and security incidents constitute breaches. Privacy and security incidents that compromise PHI are considered breaches under HIPAA.[11] States—or their contractors that are not business associates but are also covered entities—must report confirmed breaches to OCR and affected individuals.[12] Contractors that are business associates must report confirmed breaches to the applicable covered entity.[13] For breaches that affect 500 or more individuals, States and contractors also must notify the media.[14]

For example, for the nine selected breaches, States told us that they used a variety of tools to assess whether reported incidents constituted breaches under HIPAA. One State used a spreadsheet that assigned points to an incident on the basis of several key factors—e.g., how the incident occurred, the type of PHI involved, who received the PHI, and whether the PHI was returned—to help officials determine whether the incident constituted a breach under HIPAA. Other States used decision trees to guide the process or incorporated the assessment into their standardized incident-report forms.

[11] An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. To determine whether there is a low probability that the PHI has been compromised, States and/or contractors must consider the following factors: (1) the nature and extent of the PHI involved; (2) the person(s) to whom the disclosure was made; (3) whether the PHI was viewed or acquired; and (4) the extent to which the risk to the PHI was mitigated. 45 CFR § 164.402.

[12] 45 CFR §§ 164.408 and 164.404.

[13] 45 CFR § 164.410.

[14] 45 CFR §§ 164.406.

See Exhibit 5 for an example of an instance in which a Medicaid contractor determined that an incident did not constitute a breach under HIPAA.

Exhibit 5: Contractor incident that was determined, after assessment, not to constitute a Federal breach

Unauthorized access/disclosure that affected 19,987 beneficiaries. A contractor emailed a report that contained PHI to the wrong medical group.

PHI disclosed: Names and Medicaid identification numbers.

How did the State learn of the breach?
The contractor reported the breach to the Medicaid agency, which reported it to the State privacy office.

Who conducted the assessment/investigation?
The contractor determined that the disclosure did not constitute a breach under HIPAA because the medical group that received the report is a covered entity that is obligated to protect PHI. The State "did not disagree" with this assessment.

What actions were taken to protect Medicaid beneficiaries and the Medicaid program?
Once the error was discovered, the medical group gave written assurance that the list had been destroyed. No notifications were sent because the incident was determined not to constitute a breach.

What corrective actions were taken?
The contractor implemented new safeguards to better distinguish between internal and external reports. The contractor's data team will flag reports for their intended use (i.e., internal or external); scrub data from reports targeted for external use; and confirm whether certain data should be excluded from provider-specific reports.

Additional information:
The contractor worked to prevent a recurrence of the incident even though it was not determined to constitute a Federal breach.

Source: OIG analysis of nine selected breaches in 2016.

Reporting to CMS is not always a part of States' breach-response processes

Although CMS advised States in a 2006 State Medicaid Director Letter to report breaches to CMS, most States told us that they do not routinely inform CMS of Medicaid breaches that they or their contractors experience. In the 2006 letter, CMS explained the importance of the security and privacy of beneficiary information and instructed Medicaid agencies that they "should immediately report a breach, whether discovered by [an agency's] own staff or reported by a contractor" to CMS.[15] Additionally, in its 2007 response to States' questions about the State Medicaid Director Letter, CMS explained that it periodically analyzes breach data to identify possible weaknesses in States' information systems or trends in changes to States' policies on the security of their systems.[16]

[15] CMS, *State Medicaid Director Letter #06-022*. Accessed at https://downloads.cms.gov/cmsgov/archived-downloads/SMDL/downloads/SMD092006.pdf on October 2, 2018.
[16] CMS, *Letter Responding to Questions About the 2006 State Medicaid Director Letter,* August 2007.

However, in our review, States explained that they shared information about breaches with CMS in limited situations. Most often, States said that they report breaches to CMS when required to do so under data use agreements that allow them to access data or systems owned by CMS.[17] A few States said that they inform CMS about breaches that they determine to be severe or significant, such as those involving multiple States and contractors.

States have processes for protecting beneficiaries and programs and correcting vulnerabilities after a breach has occurred

States assess breaches to determine their potential impact on individual beneficiaries and programs

States consider whether breaches could result in any immediate or future harm, such as identity theft, improper billing, or damage to a beneficiary's reputation. State officials reported in interviews that their responses to breaches depend on a combination of factors, such as:

- how the breach occurred;
- the kind of PHI that was disclosed;
- who gained access to the PHI; and
- the scope of the breach; such as the number of individuals, States agencies, and/or contractors involved.

Officials from one State said that many of the breaches they experience do not involve the type of PHI that would lead to identity theft or harm. Because these breaches typically involve names and Medicaid eligibility, rather than SSNs or other identifying information, they may not raise high levels of concern that beneficiaries or programs will suffer harm. As a result, such breaches may not result in the type of intensive investigations and/or actions that follow IT hacking incidents.

States have processes for notifying beneficiaries about breaches. States and their contractors reported that they informed affected beneficiaries about breaches. In the nine breaches we examined more closely, this information came in the form of notification letters.[18] Notification letters typically were sent by the entity that experienced the breach—contractors prepared their own notification letters, which State officials typically reviewed. The notification letters provided information about the following: how the breaches occurred and the type of information they disclosed; efforts made or planned to limit the impact of the breaches and prevent similar breaches in the future; how beneficiaries could protect themselves; and where beneficiaries could get more information.

[17] These agreements require users to notify CMS when they experience a breach involving any data or system covered by the data use agreement.

[18] Under 45 CFR §§ 164.400-414, written breach notifications must include (1) a brief description of what happened, including the date of the breach; (2) a description of the PHI that was involved in the breach; (3) any steps that individuals should take to protect themselves; (4) a description of what is being done to investigate the breach, mitigate the impact, and protect against future breaches; and (5) contact procedures for individuals to ask questions or learn more.

The letters also detailed how the breaches were being investigated and/or informed beneficiaries that investigations had revealed no evidence that their PHI had been misused. Some States and contractors tailored the notification letters depending on who was affected by the breach. For example, following a breach that involved a stolen paper file, a contractor prepared different notification letter templates based on whether the breach affected a minor or adult and/or disclosed the beneficiary's date of birth. (See Appendix C for an example of one of these templates).

States reported processes for protecting beneficiaries from financial harm. Among the actions that States most commonly reported was offering beneficiaries services for credit monitoring and for protection against identity theft. States and contractors offered these services in their notification letters. For example, one of the nine breaches that we examined occurred when an email phishing attack on a contractor exposed sensitive information, including names, SSNs, dates of birth, driver's license numbers, State identification numbers, and bank account numbers. The contractor's notification letter offered free credit monitoring and identity restoration services for 1 year. See Exhibit 6 below for additional details on this breach.

Exhibit 6: Contractor offers credit monitoring to protect beneficiaries after phishing attack

Hacking/IT incident that affected 911 beneficiaries. An agency contractor—specifically, employees of a county that had a contract with the agency—exposed email passwords in a phishing attack.

PHI disclosed: Names; SSNs; Medicaid identification numbers; health plan numbers; driver's license numbers; dates of birth; health plan names; diagnoses and health conditions; medications and lab results; and home addresses.

How did the State learn of the breach?
Reported by another contractor (a Medicaid MCO) that was affected by the breach. The county did not report the breach directly to the State privacy office.

Who conducted the assessment/investigation?
The county worked with the Federal Bureau of Investigation, a police cybersecurity unit, and the State Attorney General's Office to investigate the incident and with a subcontractor to determine whether beneficiary PHI was available on the "dark web" (encrypted websites that can be hubs for illegal activities).

What actions were taken to protect Medicaid beneficiaries and the Medicaid program?
The county sent notifications to affected beneficiaries, OCR, and the media. It offered credit monitoring and identity-theft protection services for affected beneficiaries.

What corrective actions were taken?
The county reset passwords for the affected email accounts and implemented multifactor authentication for its email system.

Additional Information:
State officials reported working with county officials to ensure they understood their breach reporting obligations. The breach involved 14 different county-level departments and affected about 750,000 individuals, most of whom were not Medicaid beneficiaries.

Source: OIG analysis of nine selected breaches in 2016.

States also reported actions to help guard against Medicaid fraud.

States reported completing actions that could help limit improper Medicaid billing. Fraud could occur if stolen or lost Medicaid billing numbers are used to submit false claims to the State Medicaid program. States developed processes for monitoring Medicaid information systems—for example, to detect any attempts to bill the program using compromised Medicaid identification numbers—and for correcting beneficiary or provider information that had been compromised by a breach. For example, some States said that they have issued new Medicaid numbers and/or cards following a breach. See Exhibit 7 for another example of how one State responded to a breach and the steps it took to guard against Medicaid fraud. See Appendix B for a summary of the remaining selected breaches and the respective State and contractor responses to those breaches.

Exhibit 7: Contractor reviews systems to prevent reoccurrences

Hacking/IT incident that affected 3,400 beneficiaries. The contractor of a Medicaid MCO experienced a system intrusion and ransomware attack. **PHI disclosed: Names; SSNs; Medicaid and Medicare identification numbers; dates of birth; diagnoses and other treatment information; and home addresses.**
How did the State learn of the breach? The affected MCO reported it. **Who conducted the assessment/investigation?** The MCO and its affected contractor, along with a forensic investigator. **What actions were taken to protect Medicaid beneficiaries and the Medicaid program?** The contractor removed the ransomware and began an investigation into the incident. The MCO sent notifications to beneficiaries, OCR, and the media and offered beneficiaries credit monitoring and other identity-theft protection services. **What corrective actions were taken?** The MCO reviewed its processes to try to prevent something like this from happening again. The MCO also stated that it will not use this contractor in the future. **Additional Information:** At least three different MCOs had PHI disclosed through this attack.

Source: OIG analysis of nine selected breaches in 2016.

States and their contractors have processes for assessing the root cause(s) of breaches and correcting underlying vulnerabilities

All States' breach-response processes included investigating the underlying vulnerabilities that had allowed breaches to occur. For breaches experienced by State Medicaid agencies, all affected States reported that they conducted investigations to determine the root cause(s). For breaches experienced by contractors, States reported a variety of responses regarding investigations of root causes: leading such investigations, working with contractors on such investigations, and/or requiring contractors to conduct their own investigations. Some State officials told us that they become more involved in contractors'

breach investigations when the contractors do not have sufficient staff or capacity to investigate breaches on their own, fail to provide requested information, or provide information that appears to be questionable.

States reported that following breaches, they took—or ensured that their contractors took—a variety of corrective actions. Some of these actions included:

- training or retraining staff (e.g., reminding staff about agency policies for handling PHI);
- revising policies and procedures to address the underlying causes of breaches (e.g., adding internal checks to reduce the number of misdirected communications; shifting from paper to electronic payments to minimize the chance that paper checks would be lost or intercepted in the mail);
- restricting access to PHI (e.g., instituting two-factor authentication or encryption for devices containing PHI; tightening permissions for sensitive data); and
- correcting or modifying data programming (e.g., correcting programming errors that resulted in mail being directed to the wrong beneficiary, and that improperly exposed PHI through online accounts).

CONCLUSION AND RECOMMENDATION

State Medicaid agencies and their contractors manage sensitive information for millions of beneficiaries, and are vulnerable to breaches. In 2016, Medicaid agencies and their contractors experienced breaches that had the potential to adversely affect beneficiaries and programs. A small proportion of reported breaches, such as those that involved IT hacking, allowed unauthorized access to large amounts of Medicaid data and resulted in urgent responses from multiple agencies. Other breaches released information about only a single beneficiary, yet still required attention to limit potential harm to the beneficiaries affected. Some breaches appeared to be less concerning, such as those involving beneficiary information that was sent to the wrong medical providers. Although these breaches often warranted less intensive responses, States and their contractors still needed to consider whether these breaches compromised sensitive information.

Although most States' breach-response plans follow a common framework, the specific actions that States take vary depending on the circumstances of each breach, and any applicable State laws and requirements. This flexibility has allowed States to take additional steps when needed, such as engaging experts on information security and involving other State and Federal agencies. However, although CMS's guidance advises States to notify CMS of breaches, States reported that their processes do not include routinely sharing breach information with CMS.

Therefore, we recommend that CMS:

Reissue guidance to States about reporting Medicaid breaches to CMS

In 2006, CMS instructed States to notify CMS when States or their contractors experienced breaches of Medicaid data. CMS subsequently explained that knowing about Medicaid-related breaches can help it monitor data-security matters for Medicaid on a national level. With breach information, for example, CMS could identify Medicaid contractors that have experienced breaches across multiple States, or shared vulnerabilities affecting different contractors. CMS could also use this information to identify and share best practices for protecting Medicaid beneficiaries and programs. However, States reported that they did not routinely share information with CMS about their Medicaid breaches.

CMS should reissue guidance that clarifies its expectations for States' reporting of Medicaid breaches. States may not be aware of any existing expectation to report Medicaid breaches to CMS because of the 2009 enactment of the Breach Notification Rule, which required entities to report breaches to OCR. Updated guidance from CMS should detail the circumstances under which States should report Medicaid breaches to CMS (e.g., whether they should report all breaches, only breaches that affect more than 500 individuals, only breaches involving

hacking incidents) and where States should send these reports (e.g., to a CMS regional office or to a central office point of contact).

AGENCY COMMENTS AND OIG RESPONSE

CMS concurred with our recommendation and said that it will communicate to States the necessary procedures and circumstances for reporting Medicaid breaches to CMS. CMS said that for example, it may ask States to report only higher risk breaches or types of breaches that would be relevant to most other States. We encourage CMS to be as clear as possible in its guidance to States in defining what kinds of breaches it wants States to report—for example, what constitutes a higher risk breach, or which types of breaches would be relevant to most States.

See Appendix D for the full text of CMS's response.

APPENDIX A: Detailed Methodology

Data Collection and Analysis

We requested information and collected documentation about breaches and States' activities to (1) determine characteristics of breaches that State Medicaid agencies and their contractors experienced in 2016 and (2) examine States' responses to breaches that their employees or contractors experienced.

We collected the following data:

- list of all breaches that State Medicaid agencies and their contractors experienced in 2016;
- survey responses from all States about their breach-related activities;
- interview responses from officials from nine States regarding the breaches we selected for in-depth review; and
- documents related to the nine States' responses to the selected breaches.

Medicaid Breaches in 2016. We collected information about all breaches that Medicaid agencies and their contractors reported experiencing in 2016.[19] We defined breaches as those that meet the Federal definition of a breach. We collected this information from all 50 States and the District of Columbia (States).

For each breach, we requested the following information:

- the number of individuals affected,
- the type of information that was breached, and
- how the breach occurred.

We used this information to determine characteristics of the breaches experienced by Medicaid agencies and contractors in 2016. We summarized information that States provided about the number of people affected by each breach, grouping breaches into five categories. These categories were as follows: breaches that affected 1 individual, breaches that affected 2 to 9 individuals, breaches that affected 10 to 499 individuals, and breaches that affected 500 or more individuals. We used categories that reflected the distribution of indivduals affected by breaches. We also categorized the information that States provided about the type of PHI that was disclosed. We created the following categories to describe the type of data breached: name; Medicaid ID number or health plan ID number; date of birth; address; health or treatment information; SSN; and financial information. We analyzed this information to identify the types of PHI that were most often lost. Finally, we reviewed information that States reported about how breaches occurred and

[19] We focused our review on breaches experienced directly by Medicaid agencies and their contractors. Our analysis does not include other breaches that may have affected Medicaid beneficiaries, such as those that occurred in hospitals or provider offices.

assigned each breach to one of the categories that OCR uses in its breach-reporting portal.[20] These categories include Unauthorized Access/Disclosure, Loss, Theft, and Hacking/IT incident.

State Processes for Responding to Breaches. To examine State responses to breaches, we reviewed information that we collected through surveys and interviews. We selected nine breaches to review in more detail and interviewed States about these breaches. To examine how States responded to different types of breach scenarios, we selected breaches that reflected a variety of circumstances. We reviewed breaches that affected a single person and those that affected multiple individuals. We also selected breaches for which identifying and sensitive health information, such as patient name, diagnosis, treatment, and identification number, were disclosed. Lastly, we selected breaches that resulted from hacking, misdirected mail, theft, and loss.

We synthesized information collected through the State surveys, our in-depth reviews of breach cases, and documents from the nine States to examine how States responded to different types of breach scenarios.

[20] Office for Civil Rights. Breach Portal. Sample Form. Accessed at https://ocrportal.hhs.gov/ocr/breach/doc/Breach%20Portal%20Questions%20508.pdf;jsessionid=2CE03CE5CF3A3B1252237CA01A15C788 on March 23, 2018.

APPENDIX B: States' Responses to Nine Reported Breach Cases

The cases we examined more closely illustrate the four central activities described previously: collecting incident reports; determining or confirming whether incidents constituted breaches under HIPAA, protecting beneficiaries and programs, and correcting vulnerabilities. States' level of involvement and specific actions differed depending on a variety of factors, such as whether the breach affected State or contractor systems; resulted from hacking or human error; or affected one person or thousands. Summaries of the nine selected breaches are included below and in Exhibits 5, 6, and 7 in the findings.

Breach Case 1: Medicaid contractor mailed letter to wrong person.

Unauthorized access/disclosure that affected one beneficiary. An MCO employee mailed a beneficiary's plan of care to the wrong person.

PHI disclosed: Name; Medicaid identification number; health information, including a behavioral health diagnosis; and address.

How did the State learn of the breach?
The MCO reported it to the State privacy office.

Who conducted the assessment/investigation?
MCO officials determined that the incident was caused by human error.

What actions were taken to protect Medicaid beneficiaries and the Medicaid program?
The unintended recipient confirmed destruction of the documents received in error. The MCO sent notifications to the affected beneficiary and OCR, and offered identity protection services to the beneficiary.

What corrective actions were taken?
The MCO employee responsible for the error received training on how to handle beneficiary mail more safely.

Additional information:
The unintended recipient first alerted the MCO to the breach.

Breach Case 2: Extensive amount of documents containing sensitive information lost

Unauthorized access/disclosure that affected two beneficiaries. A package mailed by an agency employee was not received, and the package also inadvertently included information about an unrelated individual.

PHI disclosed: Names; SSNs; dates of birth; provider names and contact information; medical diagnoses; medication and prescription information; phone numbers; home addresses; and, for at least one of the beneficiaries, a Medicaid identification number.

How did the State learn of the breach?
It was reported to the State privacy office by the employee who mailed the package.

Who conducted the assessment/investigation?
The State privacy official.

What actions were taken to protect Medicaid beneficiaries and the Medicaid program?
The State privacy official sent notifications to the affected beneficiaries and OCR, and offered credit monitoring services to beneficiaries.

What corrective actions were taken?
The State privacy official reported sending emails to staff to remind them of the department's policies for handing and mailing PHI. Additionally, the office reviewed procedures for mailing documents to make this process more secure.

Additional information:
The package contained over 2,000 pages documenting a single beneficiary's medical history and eligibility for health care services. The package also inadvertently included a treatment authorization for an unrelated individual.

Breach Case 3: Information System Hacked at Business Associate of a Medicaid Managed Care Organization

Hacking/IT incident that affected about 370,000 beneficiaries. An unauthorized individual hacked into the computer server of a business associate of a Medicaid managed care organization (MCO).

PHI disclosed: Names; dates of birth; diagnosis information; and SSNs.

How did the State learn of the breach?
MCO officials reported it after the hacker notified them of the incident.

Who conducted the assessment/investigation?
The MCO and its business associate, working with forensic security investigators.

What actions were taken to protect Medicaid beneficiaries and the Medicaid program?
The MCO sent notifications to affected beneficiaries, the media, and OCR and offered beneficiaries credit-monitoring services.

What corrective actions were taken?
The MCO reported working with its business associate to increase security of PHI. The State reported making plans to strengthen breach-reporting requirements for MCOs.

Additional information:
State officials reported that the MCO had to confirm that the hacker who reported the breach was actually able to access sensitive data.

Breach Case 4: Medicaid Card Sent to Wrong Individual

Unauthorized access/disclosure that affected one beneficiary. A contractor's employee sent an enrollment package containing a Medicaid card to the wrong address because the beneficiary was improperly connected to the wrong Medicaid record.

PHI disclosed: Name and Medicaid identification number.

How did the State learn of the breach?
It was reported to the privacy office by a contractor.

Who conducted the assessment/investigation?
A State privacy official reviewed and confirmed the contractor's determination that the affected beneficiary should be notified.

What actions were taken to protect Medicaid beneficiaries and the Medicaid program?
Medicaid coverage associated with the improperly connected record was closed and reopened under the correct record. The contractor notified the affected individual and offered identity theft protection services.

What corrective actions were taken?
The employee responsible for the error was reprimanded and retrained. According to the State privacy official, the contractor also modified its data entry system to allow employees to more easily verify personal identifiers when making changes to beneficiary records.

Additional information:
The contractor experienced several similar breaches in 2016. According to the State privacy official, the contractor pressured its employees to get tasks completed faster, which led to mistakes.

Breach Case 5: Beneficiary Information Stolen From the Car of a Contractor

Theft of a paper file that affected 1,235 beneficiaries. A bag containing an encrypted laptop and a paper file was stolen from the car of a contractor's employee.

PHI disclosed: Names, dates of birth, SSNs, and Medicaid identification numbers.

How did the State learn of the breach?
Reported by the contractor's privacy official.

Who conducted the assessment/investigation?
The contractor.

What actions were taken to protect Medicaid beneficiaries and the Medicaid program?
The contractor sent notifications to beneficiaries, OCR, and the media and offered credit monitoring services to beneficiaries.

What corrective actions were taken?
The contractor updated policies for securing written, electronic, and verbal PHI taken offsite, requiring approval for employees to remove PHI or other personally identifiable information from their worksite; terminated the employee responsible for the breach; and provided additional training on safeguarding PHI to other employees.

Additional information:
State official described the challenge of imposing sanctions on a contractor that performs an essential program function, when the State has few other options available for completing this function.

Breach Case 6: Unencrypted Email sent with Beneficiary Information

Unauthorized access/disclosure that affected 12,731 beneficiaries. An agency employee sent an unencrypted email.

PHI disclosed: Names, Medicaid identification numbers, and the name and address of the adult day homes in which the beneficiaries resided.

How did the State learn of the breach?
The State agency that experienced the breach reported it to the State privacy official.

Who conducted the assessment/investigation?
The State privacy office completed the risk assessment to determine whether the incident was a breach.

What actions were taken to protect Medicaid beneficiaries and the Medicaid program?
The State agency responsible for the breach sent the notifications to the affected beneficiaries. The letter included phone numbers for credit reporting agencies, for beneficiaries who were concerned about fraudulent use of their PHI. Notifications were also sent to OCR and the media.

What corrective actions were taken?
The State agency stopped including Medicaid identification numbers in its emails.

Additional information:
Although the State's centralized privacy official might normally send notifications to affected individuals, in this case the State ensured that the letterhead reflected the State agency that experienced the breach, as that agency was better known to affected beneficiaries.

APPENDIX C: Example of a Beneficiary Notification Letter

Breach notification letters may vary, but according to 45 CFR § 164.404, each should include (1) a brief description of what happened, including the date of the breach; (2) a description of the PHI that was involved in the breach; (3) any steps that individuals should take to protect themselves; (4) a description of what is being done to investigate the breach, mitigate the impact, and protect against future breaches; and (5) contact procedures for individuals to ask questions or learn more. Below is an example of a breach notification letter illustrating each of these five elements.

[redacted]
(parent of member)
(address)
(address)

Activation Code: (#)

Dear Parent:

We are sending this letter to you as part of the [redacted] commitment to patient privacy. [redacted] is the Medicaid fiscal agent for the [redacted]. Securing your private information is very important to us at [redacted]. We want to make sure you are fully aware of a potential privacy issue.

On [redacted], [redacted] determined there had been a theft of a printed report. The information in the report is used for certain administrative functions of the [redacted] and included the following information related to your minor child:

- Medicaid Member ID
- Member Name
- Social Security Number
- Medicaid case number
- Date of birth

No other information related to your minor child was included in the report.

[redacted] internal process updates have already been implemented to ensure a similar event does not reoccur. We have no reason to believe that your minor child's information has been or will be used inappropriately. Nevertheless, out of an abundance of caution, we are extending the opportunity for you to take the steps described in this letter to protect your minor child from the possibility of fraud through identity theft. We are offering one year of credit protection service at no cost to you. In addition to the steps below, please review any explanation of medical benefits your minor child may receive and immediately report any suspicious activity to your case worker.

(1) How the breach occurred

(2) Type of PHI disclosed

(3) Efforts taken to limit the impact of the breach and prevent future breaches

Monitor your minor child's credit reports with the major credit reporting agencies:

Equifax
1-800-525-6285
PO Box 740256
Atlanta GA 30374
www.equifax.com

Experian
1-888-397-3742
PO Box 9556
Allen TX 75013
www.experian.com

TransUnion
1-800-372-8391
1561 E. Orangethorpe Ave.
Fullerton CA 92831
www.transunion.com

You are entitled to a free copy of your minor child's credit report from each of those agencies once a year. Call the credit reporting agency if you find accounts you did not open, inquiries from creditors that you did not initiate or inaccurate personal information.

We have arranged with Equifax Personal Solutions to help you protect your minor child's identity and your minor child's credit information at no cost to you. You must activate your minor child's protection within 60 days of the date on this notice. The steps to follow are:

1. Enroll in Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product. This product is being provided to you at no cost for one year.
2. Additionally, you may choose to adopt an increased level of protection by placing a fraud alert on your minor child's credit file at Equifax and the other two credit reporting agencies.

Enroll in Equifax Child Identity Monitoring

Equifax Child Identity Monitoring will scan the Equifax credit database for any instances of the minor's social security number and look for a copy of the minor's credit file.

- If no SSN match is found and no credit file exists, Equifax will create a credit file in the minor's name and immediately "lock" the credit file. This will prevent access to the minor's information in the future. If someone attempts to use your minor's information to open credit, you will receive an email alert.
- If there is a match and a credit file exists, Equifax will immediately "lock" the file, initiate an investigation into the use of that file and alert you to new attempts to use your minor's information.

How to Enroll for Parents or Guardians:

Parents or guardians – if you have not ordered from Equifax in the past, you will need to create an account with us. Please follow the instructions below. If you have questions for Equifax, you may call the phone number listed in the Equifax Member Center or in the Equifax email communication.

(4) Steps beneficiaries can take to protect themselves

To sign up please visit www.myservices.equifax.com/minor

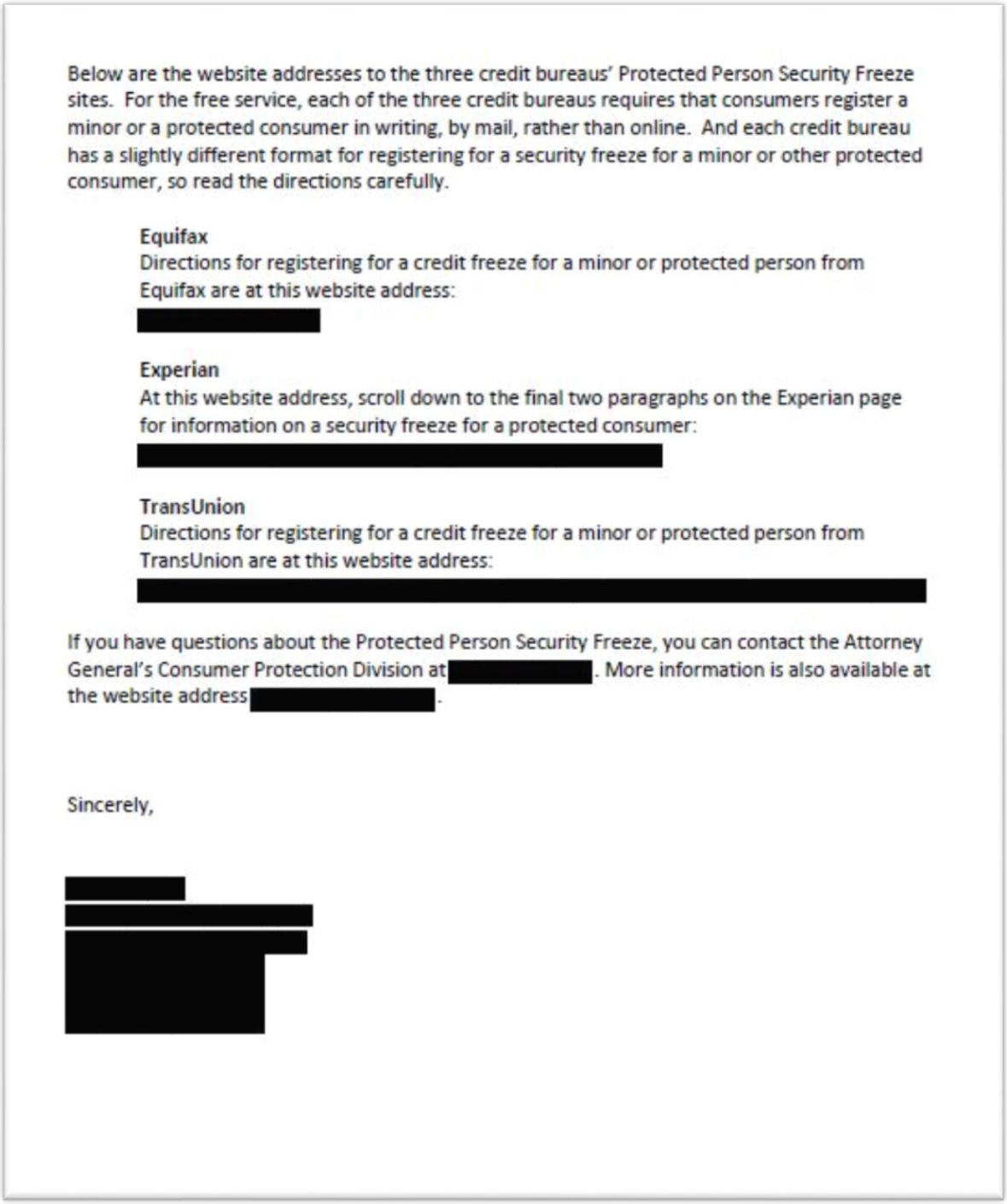
1. Below the login screen, you will see text that reads "Don't have an Equifax account? Please click here to create an account." Please click to create your account.
2. Enter in the parent/guardian information on the screens that follow in order to create an account.
3. Select the button for "$29.95 for 12 months".
4. Enter a promotion code to order the first minor product and click "apply code". This will zero out the price of the product. Do not enter credit card information.
5. Check the box to agree to the Terms of Use.
6. Next, click the "Continue" button.
7. You will be prompted to answer certain authentication questions to validate your identity.
8. Please review the order and click the "Submit" button.
9. You will then see the Order Confirmation. Please note that since you did not enter credit card information you WILL NOT be billed after the 12 months.
10. Click "View my Product" which will take you to your Member Center.
11. Click the orange button "Enroll Child" to enter your minor child's information (child's name, Date of Birth and Social Security Number). Note: if you enter the child's SSN incorrectly, you will need to remove the minor by going to your Member Center and clicking on "My Account" to remove the minor from monitoring the account. You may then re-enroll the minor with the correct SSN.
12. Check the box confirming you are the child's parent or guardian.
13. Click "Submit" to enroll your minor child.
14. If you are enrolling multiple minors, please log out, then repeat the above process to add another minor.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your minor child's credit report. This statement alerts creditors of possible fraudulent activity within your minor child's report as well as requests that they contact you prior to establishing any accounts in your minor child's name. Once the fraud alert is added to your minor child's credit report, all creditors should contact you prior to establishing any account in your minor child's name. To place a fraud alert on your minor child's credit file, visit: www.fraudalerts.equifax.com or you may contact our auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your minor child's behalf.

You may also request a security freeze. As part of an ongoing effort by the Attorney General's Office to help consumers protect themselves from identity theft and safeguard their credit, [redacted] Because identity thieves could attempt to steal the information of individuals such as children [redacted] who have clean credit history in order to assume their identities and perpetrate fraud, [redacted] offers a security freeze for protected consumers, similar to the credit freeze for adults. Parents can use it to protect their children from identity theft even if the minors don't have credit yet. [redacted]

Breach Notification Example Continued



Below are the website addresses to the three credit bureaus' Protected Person Security Freeze sites. For the free service, each of the three credit bureaus requires that consumers register a minor or a protected consumer in writing, by mail, rather than online. And each credit bureau has a slightly different format for registering for a security freeze for a minor or other protected consumer, so read the directions carefully.

Equifax
Directions for registering for a credit freeze for a minor or protected person from Equifax are at this website address:
[redacted]

Experian
At this website address, scroll down to the final two paragraphs on the Experian page for information on a security freeze for a protected consumer:
[redacted]

TransUnion
Directions for registering for a credit freeze for a minor or protected person from TransUnion are at this website address:
[redacted]

If you have questions about the Protected Person Security Freeze, you can contact the Attorney General's Consumer Protection Division at [redacted]. More information is also available at the website address [redacted].

Sincerely,

[redacted]

(5) Where beneficiaries can get more information about the breach

APPENDIX D: Agency Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: SEP 20 2018

TO: Daniel R. Levinson
Inspector General

FROM: Seema Verma
Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: States Follow a Common Framework to Respond to Breaches of Medicaid Data (OEI-09-16-00210)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General's (OIG) draft report. CMS takes its responsibility to protect and secure Medicaid beneficiary data seriously.

CMS administers the Medicaid program, a joint federal-state health program for low-income and disabled beneficiaries, which states operate primarily through either a fee-for-service delivery system or a managed care delivery system. In a fee-for-service delivery system, states make payments to participating providers for the delivery of Medicaid services to beneficiaries. In a managed care delivery system, states contract with managed care plans and require that the plans provide or arrange for a specified package of Medicaid services for enrolled beneficiaries.

States have primary responsibility for operating their Medicaid programs including responsibility for the security of all automated data processing systems involved in the administration of the Medicaid program, and the establishment of a security plan that outlines how software and data security will be maintained[1]. In addition, state Medicaid agencies are required by part 11 of the State Medicaid Manual to be in compliance with the security and privacy standards contained in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As required by HIPAA, states must have a documented process to report breaches that compromise protected health information.

In a 2006 State Medicaid Director Letter[2], CMS advised states to immediately report breaches to CMS whether discovered by state staff or reported by a contractor. However, CMS understands the need for clarifying guidance to states regarding the circumstances under which states should report Medicaid breaches to CMS.

OIG's recommendations and CMS' responses are below.

[1] 45 CFR 95.621
[2] https://downloads.cms.gov/cmsgov/archived-downloads/SMDL/downloads/SMD092006.pdf

OIG Recommendation

The OIG recommends that CMS reissue guidance to states about reporting Medicaid breaches to CMS.

CMS Response

CMS concurs with OIG's recommendation. Although states are responsible for managing their data breaches, CMS will communicate to states the necessary procedures and circumstances for reporting Medicaid breaches to CMS. For example, CMS may ask that states report to CMS only higher risk breaches, or types that would be relevant to most other states.

ACKNOWLEDGMENTS

Christina Lester served as the team leader for this study, and Camille Harper served as the lead analyst. Office of Evaluation and Inspections staff who provided support include Althea Hosein, Kevin Manley, and Christine Moritz.

This report was prepared under the direction of Blaine Collins, Regional Inspector General for Evaluation and Inspections in the San Francisco regional office, and Abby Amoroso and Michael Henry, Deputy Regional Inspectors General.

To obtain additional information concerning this report or to obtain copies, contact the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

ABOUT THE OFFICE OF INSPECTOR GENERAL

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.