Frequently Asked Questions

Q: What happened?

A: On Sunday, February 11, 2018, unknown persons broke into DDS's Legal and Audits offices in Sacramento. These offices are located in a different building than other DDS Headquarters offices. They ransacked the offices and paper files, vandalized property, stole valuables, and started a fire. The fire set off the building's sprinklers, which caused water damage to many documents and workstations. The California Highway Patrol (CHP) is currently investigating the incident.

Q: What information was in the offices?

A: The information kept in the offices were legal files, and documents collected by DDS to conduct fiscal audits of regional centers and service providers that serve individuals with developmental disabilities.

The Audits office files covered a period of ten years, and contained a variety of health and personal information:

- Names, unique state-issued client identifier numbers, service codes, units billed, service dates, and amounts paid for services to persons with developmental disabilities.
- Payroll information, including names, Social Security numbers and wages earned for some regional center and service provider employees.
- Personal information of some parents of minor children with developmental disabilities who were assessed a parental fee, and individuals who applied to work at DDS's Audits office.

The Legal office files contained information such as:

- Names, unique state-issued client identifiers, and medical records of persons with developmental disabilities.
- Miscellaneous personal information of individuals involved in legal actions.

Q: What items were stolen from the offices?

A: Twelve state-owned laptop computers were stolen, but the data on these computers cannot be accessed because they were encrypted to meet the highest federal security standards. The Department's review of its computer system confirmed the network was not accessed. All electronic files remain protected. Personal items belonging to DDS employees and some state property were also stolen.

Q: Were files containing the personal or health information stolen or removed from the offices?

A: We have no evidence those who broke in stole personal or health information from the offices. The fire and water damage to some papers, combined with the required cleanup, makes it impossible for DDS to identify with certainty what and whose information may have been compromised. Because we do not know for sure whether information was improperly viewed or accessed during the break-in, we sent a letter and issued a public notice so those individuals potentially affected are aware of what happened, and can take steps to monitor any unusual activity regarding their personal information.

Q: How many individuals are affected by the break-in?

A: Because we cannot know with certainty whether anyone's protected health information was viewed or stolen, DDS sent a letter to all individuals with a developmental disability who received services through a regional center since 2008 notifying them of the breach, approximately 582,000 individuals.

DDS also estimates the number of individuals who were employed by a regional center or service providers, parents of minor children with developmental disabilities who were assessed a fee, and applicants who applied to work at DDS's audits office to be approximately 15,000.

Q: How many vendor audits were stored in the offices?

A: Approximately 100 vendor audits were stored in the offices.

Q: How is DDS letting people know about the breach?

A: The individuals with developmental disabilities whose protected health information was located in the offices cannot be determined; therefore, DDS sent a letter to each person receiving regional center services within the past 10 years notifying him or her of the breach.

For other individuals affected by the breach, DDS is issuing a press release to major news organizations in California about the breach, and posted notice of the breach on DDS's website, http://www.dds.ca.gov/SecurityNotice. DDS will also work with regional centers to inform individuals about the breach.

Q: In addition to issuing notices, what other actions did DDS take in response to the break-in?

A: After discovering the break-in, DDS immediately launched an internal investigation, analyzed its electronic network to confirm no unauthorized individuals accessed the

network, hired outside experts to guide DDS's response, and requested a state administrative investigation. DDS also continues to cooperate with the CHP's investigation.

Q: Why is the California Highway Patrol (CHP) conducting this investigation?

A: The CHP is responsible for the safety of state buildings. State law requires DDS to report crimes occurring on state property to the CHP.

Q: What security did the offices have?

A: Electronic keycards needed to access the offices and photo IDs were issued to building employees.

Q: What will DDS do to prevent another breach?

A: DDS will enhance building security safeguards and our procedures and practices to prevent any future incidents.

Q: What can happen if my protected health information was stolen from the offices?

A: The majority of information in the offices was protected health information, not personal information such as home addresses and social security numbers. DDS has no evidence the individuals who broke in stole any of the health information. The health information located in the offices is not the type of information typically used to commit fraud. The files containing protected health information in DDS's offices did not have insurance policy or medical provider information.

Q: What if my Social Security number was on a payroll form, medical record, fee program document, or in a legal file?

A: DDS has no evidence this information was taken, but if you are concerned you can place a fraud alert on your credit files.

Q: How do I place a fraud alert?

A: You can place a fraud alert on your credit files by following the recommended privacy protection steps outlined in the Breach Help–Consumer Tips from the California Attorney General. It can be found at: https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf.

You may also contact the three credit bureaus directly:

Experian	(888) 397-3742
Equifax	(800) 525-6285

TransUnion (800) 680-7289

Q: How can I find more information about my privacy rights?

A: For more information about your privacy rights, you can visit the website of the California Department of Justice, Privacy Enforcement and Protection at: https://oag.ca.gov/privacy/medical-privacy.

Q: What can I do if I have additional questions?

A: If you have more questions about this breach, please contact DDS's call center Monday through Friday from 6:00 a.m. to 6:00 p.m., or Saturday and Sunday from 8:00 a.m. to 5:00 p.m., Pacific Time, at (877) 790-8160. You may also e-mail DDS directly with questions at SecurityBreachQuestions@dds.ca.gov. Please do not include your social security number or medical information in an e-mail to DDS.

Q: How long will the DDS call center be open?

A: The DDS call center will be open from April 7, 2018, to at least July 6, 2018.