California Department of Developmental Services

News Release

FOR IMMEDIATE RELEASE
NUMBER: 18-10
DATE: **April 6, 2018**

CONTACT: Nancy Lungren
w:(916) 654-1820
nancy.lungren@dds.ca.gov

DDS ISSUES NOTICE OF POTENTIAL BREACH OF CONFIDENTIAL INFORMATION

SACRAMENTO **--** The Department of Developmental Services today informed the public about a recent incident that may have resulted in the breach of confidential information. On February 11, a break-in occurred at the DDS legal and audits office building in Sacramento. The trespassers ransacked files, vandalized and stole state property and started a fire. The Department has no evidence that personal and health information was compromised due to the incident. However, out of an abundance of caution, it is notifying clients and the public about the incident and following federal requirements regarding potential breaches.

As detailed in the notices below, the people who broke into the building had access to the health information of about 582,000 individuals served by DDS. They also had access to the personal information of about 15,000 employees of regional centers, service providers, applicants seeking employment with the Department's audits office, and parents of minors enrolled in DDS programs.

DDS immediately notified law enforcement authorities when the incident occurred, and an investigation is ongoing.

DEPARTMENT OF DEVELOPMENTAL SERVICES
1600 NINTH STREET, Room 300, MS 3-18
SACRAMENTO, CA 95814
Toll Free (877) 790-8160

April 6, 2018 **Notice of Breach of Protected Health Information**

The Department of Developmental Services (Department) is writing to inform you about an incident that happened at the Department's legal and audits offices in Sacramento. As explained in this letter, unknown persons broke into the offices, and had access to your personal health information. We have no evidence to believe those who broke in actually stole your information or can use any stolen information to harm you. In the abundance of caution, we are providing you this notice so you are aware of what happened, and can take steps to monitor any unusual activity regarding your personal health information.

What Happened: On Sunday, February 11, 2018, unknown persons broke into the Department's legal and audits offices, ransacked the offices and paper files, vandalized property, and started a fire. The fire set-off the

building's sprinklers, which caused water damage to many documents and computer workstations. Law enforcement is investigating the incident.

After the break-in, the Department discovered a number of paper documents and compact discs (CDs) were either displaced or damaged from the fire and the sprinklers. Some of these paper documents and CDs included protected health information (PHI). Twelve state-owned laptop computers were also 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.

Please note, the Department is not aware of any evidence the PHI on the documents or CDs located in the offices were taken or viewed by the thieves, or that the PHI on those documents or CDs was compromised in any way.

What Information Was Involved: The fire and water damage to some papers, the existence of CDs, combined with the required cleanup, makes it impossible for the Department to identify with certainty whose PHI may have been compromised. Because we do not know for sure whether your PHI was improperly viewed or accessed during the break-in, we are sending you this notice.

The information contained in paper files and CDs included PHI and other information such as: (1) names; (2) unique state-issued client identifier numbers; (3) service codes; (4) units billed; (5) service dates; (6) amounts paid for services; and/or (7) medical records.

What We Are Doing: After discovering the break-in, the Department immediately launched an internal investigation, analyzed the electronic network to confirm that no unauthorized individuals accessed the network, hired outside experts to guide the Department's thorough response, and requested a state administrative investigation. The Department also continues to work with the law enforcement agency investigating the break-in.

The Department has identified, and is notifying, all individuals whose PHI may have been compromised, which is why you are receiving this letter. We are committed to protecting individuals' privacy. The Department will enhance building security safeguards and our procedures and practices, and will work towards reducing any potential risks arising from this incident and preventing any future incidents.

What You Can Do: Please keep a copy of this notice for your records for future reference in case you become aware of any unusual activity involving your confidential information.

You may 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

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

For More Information: If you have additional questions about this breach, please contact the Department'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 or visit http://www.dds.ca.gov/SecurityNotice. The Department's website will have this notice and other important information available to you in several different languages. You may also e-mail us with questions at SecurityBreachQuestions@dds.ca.gov. Please do not include your social security number or medical information in an e-mail to the Department.

I understand how important your health information is to you, and sincerely apologize for any inconvenience this incident may cause you.

Sincerely,

NANCY BARGMANN
Director

DEPARTMENT OF DEVELOPMENTAL SERVICES
1600 NINTH STREET, Room 300, MS 3-18
SACRAMENTO, CA 95814
Toll Free (877) 790-8160

April 6, 2018

Notice of Breach of Personal Information

The Department of Developmental Services (DDS) is providing this notice to the public about an incident that happened at the Department's legal and audits offices in Sacramento. As explained in this notice, unknown persons broke into the offices, and had access to personal information of employees of regional centers and service providers, applicants seeking employment with the Department's audits office, and parents of minors enrolled in DDS fee programs. We have no evidence to believe those who broke in actually stole personal information. In an abundance of caution, we are providing this public notice so those individuals potentially affected may be aware of what happened, and can take steps to monitor any unusual activity regarding their personal information.

What Happened: On Sunday, February 11, 2018, unknown persons broke into the Department's legal and audits offices, ransacked the offices and paper files, vandalized property, and started a fire. The fire set off the building's sprinklers, which caused water damage to many documents and computer workstations. Law enforcement is investigating the incident.

After the break-in, the Department discovered a number of paper documents were either displaced or damaged from the fire and the sprinklers. Some of these paper documents included personal information of employees of regional centers and service providers, applicants seeking employment with the Department's audits office, and parents of minors enrolled in DDS fee programs. Twelve state-owned laptop computers were also 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.

Please note, the Department is not aware of any evidence the personal information on the documents located in the offices were taken or viewed by the thieves, or that the personal information was compromised in any way.

What Information Was Involved: The fire and water damage to some papers, combined with the required cleanup, make it impossible for the Department to identify with certainty whose personal information may have been compromised. Because we do not know for sure whether personal information was improperly viewed or accessed during the break-in, we are issuing this public notice.

The information contained in paper files included personal information of certain employees of regional centers and service providers, applicants seeking employment with the Department's audits office, and certain parents of minors enrolled in DDS' Annual Family Program Fee, Family Cost Participation Program, or Parental Fee Program. The personal information included the following: 1) name; 2) address; 3) phone numbers; 4) social security number, and 5) financial records.

What We Are Doing: After discovering the break-in, the Department immediately launched an internal investigation, analyzed the electronic network to confirm no unauthorized individuals accessed the network, hired outside experts to guide the Department's thorough response, and requested a state administrative investigation. The Department also continues to work with the law enforcement agency investigating the break-in.

We are committed to protecting individuals' privacy. The Department will enhance building security safeguards and our procedures and practices, and will continue to work towards reducing any potential risks arising from this incident and preventing any future incidents.

What You Can Do: Please keep a copy of this notice for your records for future reference in case you become aware of any unusual activity involving your confidential information.

You may 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

Other Important Information: For additional information about your privacy rights, you may visit the website of the California Department of Justice, Privacy Enforcement and Protection at www.privacy.ca.gov.

For More Information: If you have additional questions about this breach, please contact the Department'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 or visit http://www.dds.ca.gov/SecurityNotice. The Department's website will have this notice and other important information available to you in several different languages. You may also e-mail us with questions at SecurityBreachQuestions@dds.ca.gov. Please do not include your social security number or medical information in an e-mail to the Department.

DDS understands the importance of personal information, and sincerely apologizes for any inconvenience this incident may cause.

###