DATA BREACH AT DSH-ATASCADERO

FAQ

1. What happened?

ANSWER: On February 25, 2021, it was discovered that a DSH employee with access to DSH-Atascadero data servers as part of their Information Technology job duties improperly accessed approximately 1415 patient and former patient, and 617 employee names, COVID-19 test results, and health information necessary for tracking COVID-19. On March 15, 2021, during the investigation into this incident, DSH discovered that the same employee had improperly accessed personal information, including addresses, phone numbers, email addresses, social security numbers, date of birth, and health information related to employment, of approximately 1735 employees and former employees, and 1217 DSH job applicants who never became DSH employees. On April 15, 2021, during further investigation into this incident, DSH discovered more information that the employee had improperly accessed, including addresses, phone numbers, email addresses, social security numbers, dates of birth, and driver's license numbers of 80 individuals, the date of birth and last four digits of the social security numbers of approximately 20 individuals, immigration information of 38 individuals, and health information related to employment, of approximately 81 individuals who are either employees, former employees, or DSH job applicants who never became DSH employees. At this time, DSH has no evidence that there has been any use or attempted use of the information compromised by this incident.

2. How was the data breach discovered?

ANSWER: The initial data breach was identified on February 25, 2021, as part of DSH's annual review of employees' access rights to data folders pursuant to its information and systems and access rights policy and procedure. The investigation is ongoing.

3. What kind of information was accessed?

ANSWER: On February 25, 2021, DSH discovered that the following data had been improperly accessed: names, COVID-19 test results, and health information necessary for tracking COVID-19 of patients, former patients, and employees. On March 15, 2021, as part of the ongoing investigation of this incident, DSH discovered that personal information, such as names, addresses, social security numbers, date of births, general outcome of various health-related tests done for purposes of employment with DSH, and interview and job transfer information of employees and DSH job applicants, had also been improperly accessed. On April 15, 2021, during further investigation into this incident, DSH discovered more information that the employee had improperly accessed, including addresses, phone numbers, email

addresses, social security numbers, dates of birth, and driver's license numbers of 80 individuals, the date of birth and last four digits of the social security numbers of approximately 20 individuals, immigration information of 38 individuals, and health information related to employment, of approximately 81 individuals who are either employees, former employees, or DSH job applicants who never became DSH employees. This FAQ will be updated in the event it is determined that more information was accessed. There were, on average, 1028 patients over the past 12 months, and approximately 1727 employees at DSH-Atascadero during the fiscal year 2019/2020.

4. Did the data breach happen on the same day that you learned about it? If not, when did it happen?

ANSWER: Based on the current status of the investigation, the unauthorized actions had been ongoing for about two years prior to the initial detection on February 25, 2021. The safeguards put in place by DSH's policy and procedure in relation to employee access to data files did not identify the unauthorized actions earlier because they were identical to the actions that the employee was authorized to do when performing their job functions. It is common practice for system administrators to copy files on behalf of DSH business units, which makes it challenging to automatically detect any files they might be inappropriately copied or accessed. (Please see Question #18 for steps DSH is taking to address these issues.) It appears that the employee used the access they were provided in order to perform their normal job duties to go directly into the server, copy files containing patient, former patient, and employee names, COVID-19 test results, and related health information without any apparent connection to their job duties, indicating a high probability of unauthorized access. There is also evidence that the employee viewed files containing the personal information of DSH employees and job applicants without any apparent connection to their job duties. DSH's annual audit of access rights pursuant to its information and systems access rights policy and procedure triggered this investigation and identified the unusual behavior.

5. How would I know if my information was accessed?

ANSWER: If your information was accessed you would have been notified by DSH via a Notice of Data Breach letter. The next of kin or personal representatives of deceased patients were notified by first-class mail if their address is known to DSH. If it is determined that more information was accessed than what was provided in the Notice of Data Breach letter, another Notice of Data Breach letter with relevant details will be provided to the affected individuals, or next of kin/personal representative of deceased patients, within the timeframe prescribed by law from the discovery that more information was accessed. It is possible that you will receive more than one letter due to additional information that is discovered during the ongoing investigation.

6. If my information was accessed, what should I do?

ANSWER: Keep a copy of the Notice of Data Breach letter sent to you by DSH. If the Notice of Data Breach letter states that your Social Security number was accessed, we recommend that you 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 which 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 and request all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly:

Experian (888) 397-3742

Equifax (800) 525-6285

TransUnion (800) 680-7289

You may request a copy of your medical records from the DSH-Atascadero Health Information Management Department, PO BOX 7001, Atascadero, CA 93423. If you are a patient, or former patient, you may use the DSH 6406 enclosed with the Notice of Data Breach letter and submit the form to DSH for review/approval. If you are an employee, you may request your employee health information from your Return to Work Coordinator at 805-468-2307.

If you have additional questions about this breach, please contact DSH's call center Monday through Friday from 8:30 a.m. to 5:00 p.m., Pacific Time, at (844) 227-9333, or visit https://www.dsh.ca.gov/Breach_Notice.html. DSH'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 breach2021@dsh.ca.gov. Please do not include your social security number or medical information in an e-mail to DSH.

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.

DSH Patients and former patients may also contact their Patients' Rights Advocate, Lucas Campo, at (805) 468-2601, or his secretary Kathy Kalem, at (805)468-3031, with questions related to patients' rights. Employees may contact the Employee Assistance Program (EAP), for support services at www.eap.calhr.ca.gov.

7. What was done with the accessed information?

ANSWER: At this time, DSH has no evidence that there has been any use or attempted use of the information compromised by this incident. DSH is continuing to monitor closely for any such activity.

8. Is it possible that more information was accessed than you know about right now? When will you know?

ANSWER: Investigators continue to seek more information about the extent of the data breach. If it is determined that more information was accessed than what was provided in the Notice of Data Breach letter, another notification will be provided to the effected individuals within the timeframe prescribed by law from the discovery that more information was accessed.

9. Who did it?

ANSWER: DSH is investigating the breach and has placed the principal subject of the investigation on administrative leave pending completion of the investigation.

10. Is the person who did it still working at DSH?

ANSWER: DSH is investigating the breach and has placed the principal subject of the investigation on administrative leave pending completion of the investigation.

11. Was the data breach intentional?

ANSWER: Whether the data breach was intentional is currently unknown. Investigators continue to seek more information about the data breach including the actions that led to it.

12. Do you know why someone did this?

ANSWER: The reason why the individual improperly accessed files is currently unknown. Investigators continue to seek more information about the data breach including the actions that led to it.

13. Why didn't you tell us about this sooner?

ANSWER: The investigation involves manual reviews of all electronic files accessed by the employee, a determination as to whether access was authorized or not, restoration of the improperly accessed files to the date they were accessed, and compilation of the individuals and information impacted, all of which takes time. Impacted individuals were informed within the timeframe prescribed by law from the discovery of the breach in compliance with state and federal laws.

14. Does my union know about this?

ANSWER: DSH employee labor representatives have been provided with a courtesy copy of the Notice of Data Breach that were given to impacted individuals.

15. How often does DSH look for data breaches?

ANSWER: The DSH Privacy and Security Programs review, investigate, and analyze privacy incidents on a daily basis for potential data breaches pursuant to its information and systems and access rights policy and procedure and incident response plan. Additionally, DSH monitors employee access rights to data folders annually, and administrative account access quarterly, to ensure role-based access is maintained for confidential information pursuant to its information and systems and access rights policy and procedure.

16. Is the search for data breaches automated, manual or something else?

ANSWER: The search for data breaches is both an automated and manual process. DSH employs automated Data Loss Prevention techniques in an effort to eliminate data being transmitted externally from the Department. A manual process for detection is also utilized, as many DSH employees require access to confidential data as a normal part of their jobs, including copying and moving data between systems internally.

17. Is there a policy for looking for data breaches and, if so, was it followed?

ANSWER: DSH has a Privacy and Security incident response plan that was followed in this incident.

18. What are you doing to make sure that this doesn't happen again?

ANSWER: Backup administrators who supported primary administrators with specific functions less frequently have been eliminated, and all administrative activities will be logged and monitored on a more detailed basis. Review of administrator access and activity will be conducted more frequently to ensure that access is being conducted appropriately. Automated detection mechanisms will be tightened to detect transfer of PII and PHI to locations which do not typically store PII and PHI. Senior management approval has been added to any administrator access, and the review of access will be conducted more frequently. Existing mandatory security and privacy training will be expanded to encompass additional scenarios.

19. Who has been notified about the breach?

ANSWER: In addition to the notifications provided to patients, former patients, former and current employees, and job applicants affected by the breach, the breach was reported to the United States Health and Human Services, Office of Civil Rights, the California Office of Information Security, the California Office of Health Information Integrity, the California Highway Patrol, the California Department of Public Health, and the California Attorney General's Office as required by law.