JOSH GREEN, M.D.
GOVERNOR OF HAWAI'I
KE KIA'ĀINA O KA MOKU'ĀINA 'O HAWAI'I

KENNETH S. FINK, MD, MGA, MPH
DIRECTOR OF HEALTH
KA LUNA HO'OKELE

STATE OF HAWAI'I
DEPARTMENT OF HEALTH
KA 'OIHANA OLAKINO
P. O. BOX 3378
HONOLULU, HI 96801-3378

In reply, please refer to:
File:

March 3, 2023

The Honorable Scott K. Saiki
Speaker of the House of Representatives
Members of the Hawaii State House of Representatives
Thirty-Second State Legislature
Hawaii State Capitol
415 S. Beretania Street
Honolulu, Hawaii 96813

Dear Speaker Saiki and Members of the House of Representatives:

In accordance with Section 487N-4, Hawai'i Revised Statutes, this letter shall serve as our report to the Legislature concerning a security breach of the Hawai'i State Department of Health Electronic Death Registry System.

Incident

- On January 2023, 1:20 p.m. HST, Mandiant, a cybersecurity threat intelligence company, notified Enterprise Technology Services (ETS) and the Hawai'i State Department of Health (HDOH) that an external medical certifier account of the Electronic Death Registry System (EDRS) was compromised and placed for sale on the dark web (internet marketplace where cybercriminals can transact illegal products and services).
- The medical certifier account role can certify a death, create a new case, and certify/print a death worksheet. The role cannot print a death certificate.
- At 2:26 p.m. HST, the compromised medical certifier account was identified. The account was immediately disabled, locked, and the password was changed.
- At 3:00 p.m. HST, HDOH immediately met with ETS and NIC Hawai'i (vendor for EDRS system) to discuss the incident, identify steps to correct the issue, and provide recommendations to prevent this type of incident from reoccurring.
- NIC Hawai'i began reviewing relevant system logs and application data to investigate the compromised account.
    - The compromised account was a former Tripler Hospital medical certifier who left the organization in 2021. The account remained in the EDRS system, as HDOH was unaware of the user no longer being part of the organization.

  - The compromised account was successful in authenticating from two IP addresses in 1) Somerset, Kentucky, and 2) Naaldwijk, South Holland, Netherlands.
  - Initial login by the bad actor using the compromised account was on 1/20/2023, 2:30 a.m. HST.
  - Last login by the bad actor using the compromised account was on 1/23/2023, 10:33 a.m. HST.
  - 3,402 death records may have been viewed by the bad actor.
    - Data fields that could be viewed include Name, Social Security Number, Address, Sex, Date of Birth, Date of Death, Place of Death, Cause of Death and Certifier of Death.
    - 3,048 of the death records were for individuals who died in 2014 or earlier.
    - 3,372 records had previously been certified and cannot have any information changed as the record is locked from any updating.
    - The 30 records that had not been certified were reviewed, and the bad actor did not certify any of them.
- NIC Hawai'i completed its investigation and consultation with its legal corporation counsel and issued its final report of the incident on February 15, 2023.

Root Cause

- A bad actor compromised an account from a former employee of an external organization.
- The compromised account was not used since 2021.
- External user accounts were not properly disabled after an employee was terminated.

Corrective Action

- A list of users was provided to the external organization for review so it could identify employees who were no longer with the organization. HDOH removed these identified accounts from the EDRS system.
- More complex passwords will be enforced to enhance secure access to the application. Passwords must be 10 characters in length and must include a combination of a lowercase letter, uppercase letter, number, and a special character.
- Passwords that were previously used cannot be used for six iterations.
- User accounts that have not been accessed for 90 days will be disabled.
- External organizations using the EDRS system must promptly notify the HDOH when the organization's staff members are terminated or leave employment, so user account access can be disabled in a timely manner.

- All external organization user accounts have been notified that passwords must be changed as part of HDOH's ongoing security enhancements. A password change help desk has been established to assist users if needed on the password change process.
- A self-service password reset portal has been developed to allow users to reset passwords without contacting the HDOH.
- New accounts will be created without setting a password. The new user will use the password reset feature to create a password.
- All users will be required to change their passwords on a regular basis, that is based on a system setting controlled by the HDOH.
- Implement Multifactor Authentication for all user account access.
- All HDOH applications that have external organization user access are being reviewed so that similar changes can be applied to these systems, to prevent user accounts from being compromised.

The actions described above will prevent this type of incident from recurring. We are confident that the enhanced security changes and procedures will be effective in protecting our information technology systems.

Included with this report is the template for the notice that is being mailed to the contacts we have in our system, which may include the surviving spouse and/or the individual who reported the death to the mortuary. We included in the notice a phone number the person can call with questions.

Please contact me if you have any questions.

Sincerely,

Kenneth S. Fink, MD, MGA, MPH
Director of Health

Enclosure

<<contact name>>
<<contact address line 1>>
<<contact address line 2>>

Aloha. I am writing to notify you of an incident of unauthorized access to the Department of Health Electronic Death Registry System. The death record for <<decedent name>> may have been viewed, and you are receiving this notice because you are listed in our system as the surviving spouse and/or the person who reported the death to the mortuary.

The unauthorized access occurred because someone obtained the login credentials of a former medical certifier at a local hospital. The medical certifier had left employment at the hospital in June 2021, but the account had not been deactivated. Upon learning on January 23, 2023 that these login credentials were compromised, we immediately disabled the account and began an investigation.

Our investigation was completed on February 15, 2023 and determined that approximately 3,400 death records may have been viewed on January 20, 2023. The death records had a date of death ranging from 1998 to 2023, with 90% occurring in 2014 or earlier. Records that had been certified could not be altered, and 99% of the records had been certified. We reviewed the 1% of records that had not been certified, and none were certified by the unauthorized user.

No death certificates were accessed nor were any able to be generated. Although not downloadable, the death records themselves may have been viewed. Each contains the decedent's name, social security number, address, sex, date of birth, date of death, place of death, and cause of death. We encourage you to remain vigilant with regard to any remaining unsettled matters such as accounts, estate, life insurance claim or Social Security survivor benefits.

In response to this incident, we are in the process of expeditiously implementing new security measures for Electronic Death Registry System external accounts, including a requirement for more complex passwords, multifactor authentication, and automatic account disabling following a period of inactivity. We are also conducting a security review of external accounts for all of our systems.

If you have questions, you can call (808) 586-4462. I apologize that this incident occurred.

Me ka ha'a ha'a,

Kenneth S. Fink

JOSH GREEN, M.D.
GOVERNOR OF HAWAI'I
KE KIA'ĀINA O KA MOKU'ĀINA 'O HAWAI'I

KENNETH S. FINK, MD, MGA, MPH
DIRECTOR OF HEALTH
KA LUNA HO'OKELE

STATE OF HAWAI'I
DEPARTMENT OF HEALTH
KA 'OIHANA OLAKINO
P. O. BOX 3378
HONOLULU, HI 96801-3378

In reply, please refer to:
File:

March 3, 2023

The Honorable Ronald D. Kouchi
President of the Senate
Members of the Hawaii State Senate
Thirty-Second State Legislature
Hawaii State Capitol
415 S. Beretania Street
Honolulu, Hawaii 96913

Dear Senate President Kouchi and Members of the Senate:

In accordance with Section 487N-4, Hawai'i Revised Statutes, this letter shall serve as our report to the Legislature concerning a security breach of the Hawai'i State Department of Health Electronic Death Registry System.

Incident

- On January 2023, 1:20 p.m. HST, Mandiant, a cybersecurity threat intelligence company, notified Enterprise Technology Services (ETS) and the Hawai'i State Department of Health (HDOH) that an external medical certifier account of the Electronic Death Registry System (EDRS) was compromised and placed for sale on the dark web (internet marketplace where cybercriminals can transact illegal products and services).
- The medical certifier account role can certify a death, create a new case, and certify/print a death worksheet. The role cannot print a death certificate.
- At 2:26 p.m. HST, the compromised medical certifier account was identified. The account was immediately disabled, locked, and the password was changed.
- At 3:00 p.m. HST, HDOH immediately met with ETS and NIC Hawai'i (vendor for EDRS system) to discuss the incident, identify steps to correct the issue, and provide recommendations to prevent this type of incident from reoccurring.
- NIC Hawai'i began reviewing relevant system logs and application data to investigate the compromised account.
    - The compromised account was a former Tripler Hospital medical certifier who left the organization in 2021. The account remained in the EDRS system, as HDOH was unaware of the user no longer being part of the organization.

  - The compromised account was successful in authenticating from two IP addresses in 1) Somerset, Kentucky, and 2) Naaldwijk, South Holland, Netherlands.
  - Initial login by the bad actor using the compromised account was on 1/20/2023, 2:30 a.m. HST.
  - Last login by the bad actor using the compromised account was on 1/23/2023, 10:33 a.m. HST.
  - 3,402 death records may have been viewed by the bad actor.
    - Data fields that could be viewed include Name, Social Security Number, Address, Sex, Date of Birth, Date of Death, Place of Death, Cause of Death and Certifier of Death.
    - 3,048 of the death records were for individuals who died in 2014 or earlier.
    - 3,372 records had previously been certified and cannot have any information changed as the record is locked from any updating.
    - The 30 records that had not been certified were reviewed, and the bad actor did not certify any of them.
- NIC Hawai'i completed its investigation and consultation with its legal corporation counsel and issued its final report of the incident on February 15, 2023.

Root Cause

- A bad actor compromised an account from a former employee of an external organization.
- The compromised account was not used since 2021.
- External user accounts were not properly disabled after an employee was terminated.

Corrective Action

- A list of users was provided to the external organization for review so it could identify employees who were no longer with the organization. HDOH removed these identified accounts from the EDRS system.
- More complex passwords will be enforced to enhance secure access to the application. Passwords must be 10 characters in length and must include a combination of a lowercase letter, uppercase letter, number, and a special character.
- Passwords that were previously used cannot be used for six iterations.
- User accounts that have not been accessed for 90 days will be disabled.
- External organizations using the EDRS system must promptly notify the HDOH when the organization's staff members are terminated or leave employment, so user account access can be disabled in a timely manner.

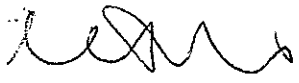
- All external organization user accounts have been notified that passwords must be changed as part of HDOH's ongoing security enhancements. A password change help desk has been established to assist users if needed on the password change process.
- A self-service password reset portal has been developed to allow users to reset passwords without contacting the HDOH.
- New accounts will be created without setting a password. The new user will use the password reset feature to create a password.
- All users will be required to change their passwords on a regular basis, that is based on a system setting controlled by the HDOH.
- Implement Multifactor Authentication for all user account access.
- All HDOH applications that have external organization user access are being reviewed so that similar changes can be applied to these systems, to prevent user accounts from being compromised.

The actions described above will prevent this type of incident from recurring. We are confident that the enhanced security changes and procedures will be effective in protecting our information technology systems.

Included with this report is the template for the notice that is being mailed to the contacts we have in our system, which may include the surviving spouse and/or the individual who reported the death to the mortuary. We included in the notice a phone number the person can call with questions.

Please contact me if you have any questions.

Sincerely,



Kenneth S. Fink, MD, MGA, MPH
Director of Health

Enclosure

<<contact name>>
<<contact address line 1>>
<<contact address line 2>>

Aloha. I am writing to notify you of an incident of unauthorized access to the Department of Health Electronic Death Registry System. The death record for <<decedent name>> may have been viewed, and you are receiving this notice because you are listed in our system as the surviving spouse and/or the person who reported the death to the mortuary.

The unauthorized access occurred because someone obtained the login credentials of a former medical certifier at a local hospital. The medical certifier had left employment at the hospital in June 2021, but the account had not been deactivated. Upon learning on January 23, 2023 that these login credentials were compromised, we immediately disabled the account and began an investigation.

Our investigation was completed on February 15, 2023 and determined that approximately 3,400 death records may have been viewed on January 20, 2023. The death records had a date of death ranging from 1998 to 2023, with 90% occurring in 2014 or earlier. Records that had been certified could not be altered, and 99% of the records had been certified. We reviewed the 1% of records that had not been certified, and none were certified by the unauthorized user.

No death certificates were accessed nor were any able to be generated. Although not downloadable, the death records themselves may have been viewed. Each contains the decedent's name, social security number, address, sex, date of birth, date of death, place of death, and cause of death. We encourage you to remain vigilant with regard to any remaining unsettled matters such as accounts, estate, life insurance claim or Social Security survivor benefits.

In response to this incident, we are in the process of expeditiously implementing new security measures for Electronic Death Registry System external accounts, including a requirement for more complex passwords, multifactor authentication, and automatic account disabling following a period of inactivity. We are also conducting a security review of external accounts for all of our systems.

If you have questions, you can call (808) 586-4462. I apologize that this incident occurred.

Me ka ha'a ha'a,

Kenneth S. Fink