Provider Directory security briefing

Jason Miranda, OHA

Oregon Health Authority

Provider Directory

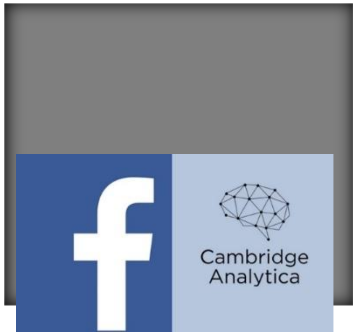
Oregon's Statewide Provider Directory

Provider Directory : Protecting Your Data

The Oregon Health Authority (OHA) and its vendors take securing the privacy and security of both the Provider Directory users and their data very seriously. OHA worked with internal privacy and security staff as well as with external stakeholders to develop program and operational requirements and guidelines that serve to safeguard the private information of users and their data from external threats that might seek to obtain it.

Cambridge Anaylitica and Facebook Scandal - Involves the collection of personally identifiable information (PII) of up to 87 million Facebook users which was used to inappropriately target individuals for ads and misinformation by 3rd parties

- ❖ Root Cause - Facebook platform was developed with poor user privacy provisions and provided poorly protected query tools that allowed any user with a Facebook account to mine PII from the platform.
- ❖ Risk/Mitigation - The Provider Directory is a closed system where access is provided only to authorized users who are vetted and verified by the program. Users and their organizations are monitored for suspicious behavior and access to data follows the "least necessary access to perform business function" methodology recommended by industry professionals. Particularly sensitive data is restricted to only certain users who have applied for and been approved to access it by OHA.

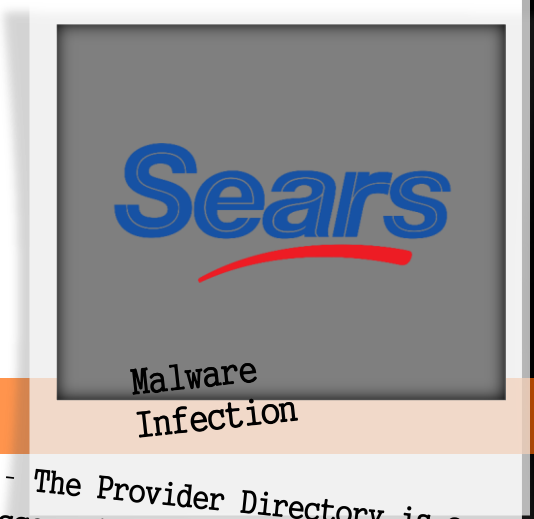


Bad Security Decisions

What not to do

How we do it right

Sears/Delta/Best Buy Data Breach - Hackers accessed several hundred thousands of the aforementioned businesses customer data including names, addresses, credit card numbers, CVV numbers, and credit card expiration dates.



Malware Infection

❖ OSPD Risk/Mitigation - The Provider Directory is a closed system where access is provided only to authorized users who are vetted and verified by the program. Particularly sensitive data is restricted to only certain users who have applied for and been approved to access it by OHA.

❖ Root Cause - Facebook platform was developed with poor user privacy provisions and provided poorly protected query tools that allowed any user with a Facebook account to mine PII from the platform

Nope

That's more like it!

EQUIFAX BREACH

- 143 MILLION AMERICANS
- NAMES, ADDRESSES
- SOCIAL SECURITY NUMBERS

Publically Accessible

Boo!

Yay!

Equifax Breach - Multiple 3rd parties located an unintentionally public facing portal intended for use by Equifax employees. 3rd parties were able to query and collect data about Americans including their names, social security numbers, birth dates, credit history, and demographics. Additionally Equifax suffered from additional breaches of similar information related to their Apache Struts platform and a known vulnerability they waited 6 months to patch.

Root Cause - Public access to internal tools and interfaces with access to consumer data was certainly the cause of the initial breach. Additionally, failure to promptly patch known platform vulnerabilities as well as storage of customer data in unencrypted or partially unencrypted formats contributed to the ease in which the data was obtained.

OSPD Risk/Mitigation - No components of the Provider Directory are available for use by users or internal staff over unauthenticated or public interfaces. Additionally, access to data is protected using industry standard access and security protocols and practices. Finally customer data is always encrypted in motion and at rest.

Provider Directory Security Approach In Review

- Access to the Provider Directory is available only through the latest HTTPS encrypted and TLS 1.2 compliant web browser interfaces
- Single Sign On Solution for practitioners provides security and convenience as well as enforcement of Security Assertion Markup Language (SAML) tokens for authentication and Multi-Factor Authentication
- All organizations are reviewed and vetted prior to being granted access to the solution and are able to self-manage user populations
- All data for Oregon customers are segregated from other platform customers and are always encrypted in motion and at rest

- Vendor is compliant with all state identity and theft protection requirements, data retention policies, and federal and state privacy and security requirements and administrative rules
- All security related technology, training, and policies are verified by an independent 3rd party evaluator yearly and by OHA and or their designees per release and quarterly
- OWASP Top 10 Compliant App Scans are performed and assessed before each new release of the solution
- Strong Service Level Agreement (SLA) provisions are in place related to data protection, breach reaction, and resolutions to ensure compliance

MiHIN and Salesforce Security and Compliance Certifications

AICPA Service Organization Control Reports℠
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

FR FedRAMP

ISO 27001
CERTIFIED
by schellman

CSA STAR

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

HIPAA

TRUSTe
VERIFIED

PCi Security Standards Council™

ISO 27018
by schellman

How does OSPD respond in the unlikely scenario of a security event?

Alert - Vendor notifies OHA within one hour of discovery, and consult with the OHA regarding procedures for providing the required notice(s)

Stop - Vendor terminates or restricts the access of any users, user accounts, or user services and interfaces associated with the breach (within 24 hours)

Notify - OHA begins the established state process of analyzing the breach, determining and correcting the fault, and notifying those effected

Questions? Comments? Applause?