OREGON PROVIDER DIRECTORY

Oregon Health Authority

Oregon Provider Directory (OPD): Privacy and Security Policies and Standards

The Oregon Health Authority (OHA) and its vendors are committed to maintaining the privacy of provider data managed and maintained by the OPD (Provider Data) and the security of the OPD system (System). OHA meets this commitment by implementing the following policies and procedures:

- Access is only provided to healthcare entities and associated staff that have signed legal agreements for proper use of the System and Provider Data
- Provider Data may only be for uses related to managing local directories, health information exchange, and analytics. Redistributing, selling, or using Provider Data for any other purpose is strictly prohibited
- Access to the System is available only through the latest HTTPS encrypted and TLS 1.2 compliant web browser interfaces
- Data for Oregon customers are segregated from other platform customers
- Data are always encrypted using AES 256 encryption for data in motion and at rest
- The Oregon Provider Directory vendor, MiHIN, must comply with and follow state identity and theft protection requirements, data retention policies, and federal and state privacy and security requirements and administrative rules including:
    - Oregon's Identity Theft Protection Act (SB 583): https://olis.leg.state.or.us/liz/2017R1/Downloads/MeasureDocument/SB583
    - Data Retention per Oregon Administrative Rule 166-300: http://arcweb.sos.state.or.us/pages/rules/oars_100/oar_166/166_300.html
    - Federal and State Privacy and Security Requirements such as those specified in HITECH, FIPS-199, FIPS 140-2, NIST 800-53, 2013 ORS Vol. 14 Chapter 646A.604, FISMA, and any others as required to facilitate certification and compliance set forth by governing bodies for web-based Provider Directory technologies.
- OHA and/or its designees and an independent third-party evaluator verifies MiHIN has met its requirements for all security related technology, training, and policies annually and per release
- OWASP Top 10 Compliant App Scans are performed and assessed before each new release of the solution
- All backups of data meet the following timeframes:

- the maximum tolerable downtime for the System or the recovery time objective (RTO) is 24 hours

- the minimum backups or recovery point objective (RPO) for databases is 2 hours; the minimum for files is 24 hours