How are FPAR data kept safe?

The Family Planning Annual Report (FPAR) is the only source of annual uniform reporting by all Title X family planning service grant recipients funded by the U.S. Department of Health and Human Services' (HHS) Office of Population Affairs (OPA). Reported to OPA for many years as aggregate data, FPAR transitioned to encounter-level data reporting from 2022 to 2024. As of January 2025, all Title X grant recipients are required to report FPAR 2.0 encounter-level data. Encounter-level data improve data collection, reporting, and analysis and better describe the services Title X delivers. Grant recipients can then use the report's information to improve access and the quality of Title X services.

Client confidentiality, a pillar of the Title X program, is built into all aspects of FPAR 2.0's development, data collection, and operations. Several layers of security operate in a system of checks and balances to protect the data submitted to OPA. Under FPAR 2.0, grant recipients report many of the same data elements they did in FPAR 1.0, but with additional context provided through encounter-level data. Before OPA collected any FPAR 2.0 data elements, all aspects of the data collection were reviewed, analyzed, and approved by federal offices governing privacy, information collection, cybersecurity, and other related IT and data security areas. Now that it is live, the FPAR system must be scanned weekly for compliance and vulnerabilities that are managed by a trained and certified federal cybersecurity professional. OPA also works with the contractors, HHS, and federal partners to maintain the confidentiality, integrity, and availability of the system.

How does OPA keep FPAR data safe?

The individual elements cleared for FPAR 2.0 data collection[1] do not contain direct personal identifiers (such as name, Social Security number, or driver's license number), therefore FPAR 2.0 encounter records cannot be linked to a specific individual. Data elements that might be used to identify patients, such as patient ID, date of birth, or date of service, are altered or hashed before being stored in the FPAR system. The information that grant recipients submit is changed in a way that prevents someone from recovering the original data elements that could identify someone or an individual encounter. OPA securely destroys grant recipient-submitted data annually.

How do OPA contractors keep FPAR data safe?

OPA contractors develop, operate, and maintain the FPAR 2.0 system under the guidance and supervision of OPA, HHS, and the federal government. These contractors must protect the confidentiality, integrity, and availability of FPAR data in accordance with HHS and federal policies. They must report any incident (or even any suspected incident) involving the following to the HHS Computer Security Incident Response Center and OPA within 24 hours:

- Cybersecurity and privacy threats
- Viruses
- Malicious activity
- Loss of unauthorized disclosure, or destruction of data

Contractors cannot sell or use these data without written permission from the government, and any unauthorized disclosure is subject to HHS sanction and potential criminal charges. In addition, every

government contractor must adhere to HHS and federal policies, including the HHS Rules of Behavior; all government contracts that have an IT component must be written in compliance with the Technology Procurement Security and Privacy Language; and the IT equipment used to host and house the information system must meet supply chain risk management requirements.

How does HHS keep our data safe?

OPA and FPAR are governed by HHS IT processes that ensure the confidentiality, integrity, and availability of all the data and information in the FPAR system. The Enterprise Performance Lifecycle[2] guides these processes, which include review and approval by the HHS Privacy Officer, HHS IT Compliance Management, HHS Enterprise Architecture, HHS Vulnerability Response Management, HHS Risk Management, Records Management, and a third-party security assessment. If FPAR passes all the checks, the HHS Chief Information Security Officer signs and issues a three-year Authority to Operate. OPA and HHS are further subject to federal policies and regulations regarding data security and IT systems.

How does the federal government keep our data safe?

HHS, OPA, and FPAR must adhere to all federally mandated IT regulations, standards, policies, procedures, and rules to protect FPAR data and FPAR system integrity. These are enshrined in laws such as the Federal Information System Modernization Act[3] or the National Cybersecurity Protection Advancement Act.[4] OPA conforms with policies, standards, and guidance developed by offices such as the Department of Commerce's National Institutes of Standards and Technology[5] and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. All OPA systems must use a cloud-service provider approved by the Federal Risk and Authorization Management Program, which provides a standardized approach to security authorizations.

Additional information

Although organizations might have experience creating data-sharing agreements for these types of data, these agreements are not required for Title X grant recipients. The type of data reported to FPAR does not include personal identifiers, and it is protected by multiple layers of security. In addition, FPAR reporting is required as a condition of accepting Title X grant funding and included in the Notice of Award.

Grant recipients and vendors can contact FPARSupport@mathematica-mpr.com with questions about FPAR. Grant recipients should also reach out to their OPA Project Officer with questions.

---

[1] FPAR 2.0 received OMB clearance under OMB control number 0990-0479. Expires 9/30/2028.

[2] Policy for Information Technology Enterprise Performance Life Cycle. Office of the Chief Information Officer (2022).

[3] Federal Information Security Modernization Act of 2014. Pub. L. No. 113-283 (2014).

[4] National Cybersecurity Protection Advancement Act of 2015. H.R. 1731 (2015).

[5] Cybersecurity and Privacy Reference Tool. National Institute of Standards and Technology (2023).