



TECHNICAL BRIEF · BASED ON GAO-24-106638 · HHS

15 OF 68 HHS PANDEMIC SYSTEMS WITH PII HAD NO PRIVACY ASSESSMENT

15 of 68

HHS PANDEMIC SYSTEMS THAT COLLECT AND STORE PII BUT HAD NO PRIVACY IMPACT ASSESSMENT

In September 2024, GAO found that 15 of the 68 HHS pandemic systems holding personal data had no privacy impact assessment, and one lacked a current ATO. Eight recommendations are closed. Two aimed at CDC remain open as of GAO's December 2025 update.

THE FINDING

In September 2024, GAO published [COVID-19: HHS Needs to Identify Duplicative Pandemic IT Systems and Implement Key Privacy Requirements](#) (GAO-24-106638). GAO and HHS component agencies identified 99 systems that support pandemic preparedness and response, and the components reported that 68 of them collect and store personally identifiable information (PII). Privacy impact assessments (PIAs) existed for 53. The other 15 had none.

GAO then sampled nine of the 99 systems at random. All nine had privacy continuous monitoring, and eight had an authorization to operate (ATO). The gaps sat elsewhere. Three security categorizations had not been reviewed and approved by the senior official for privacy, and three systems lacked a privacy control assessment.

The Electronic Medical Records System had no evidence of a current ATO. Its ATO expired in May 2024. ASPR asked for an extension in February 2024, and as of July 2024 it was still unapproved. GAO cautioned that the sample of nine is not generalizable to all of HHS.

GAO made 14 recommendations to HHS. This brief covers the ones about PIAs, categorization review, and the ATO.

WHY IT KEEPS HAPPENING

GAO's account puts the gap in documentation decisions. Seven of the 15 systems without PIAs belonged to CDC, seven to FDA, and one to ASPR.

GAO recorded the reasons for CDC's seven. Three were said to be covered by other systems' PIAs that did not mention them. Three were said not to need one because of a cooperative or data use agreement, though CDC had identified them as collecting PII. For the last, CDC offered no evidence of a PIA.

Categorization lacked a record too. CDC had categorized the COVID-19 Clearinghouse and HHS Protect, but the senior official for privacy had not reviewed or approved either.

Expiry tracking is the third thread: one system passed its ATO date while an extension request sat unapproved.

WHY IT MATTERS TO YOUR BID

Any A&A contractor taking over a system inherits its documentation state as found. GAO-24-106638 reads as a checklist of what an authorization package for a PII-bearing system should already show: a PIA, a reviewed categorization, a privacy control assessment, and a current ATO.

Three requirement types follow. An understanding-of-the-requirement section should treat privacy documentation as part of authorization, not a side task for the privacy office. A transition plan should inventory existing PIAs, categorization memos, and ATO dates in the first weeks of performance, and the approach to inherited controls should check the provider's actual package rather than assume coverage.

GAO found the same pattern at FDA: controls said to be inherited that the system's assessment report never mentioned. A proposal that names how it verifies inheritance answers that question early.

TECHNICAL APPROACH

The method below comes from Avalon's [ATO Process Facilitation service](#), delivered along the NIST SP 800-37 Rev. 2 risk management steps. It describes how the work is done, at the methodology level. The agency's authorizing official decides on the ATO and its privacy office approves PIAs; Avalon prepares the package.

1. **Run a privacy threshold analysis per system.** Record, system by system, whether PII is collected or stored and whether a current PIA exists. The register separates three states GAO found: PIA on file, PIA claimed through another system, and PIA waived by agreement. Each needs a document behind it.
2. **Draw the boundary and the data flows.** Use the authorization boundary description and network and data-flow diagrams to test "covered by another system's PIA." If PII moves into a system the cited PIA never mentions, the diagram shows it before an assessor does. PIA support artifacts go on the agency privacy office's templates.
3. **Write the FIPS 199 categorization memo for review.** Map information types under NIST SP 800-60, record the impact rationale, and route the memo with a signature block for the senior official for privacy. The approval record lives in the GRC system of record.
4. **Build the security plan and verify inheritance.** Write control implementation statements that describe what is configured, traced to a named artifact or interview. For inherited controls, check the provider's customer responsibility matrix and package. Structure the plan on [NIST SP 800-18 Rev. 2](#), finalized June 30, 2026, which treats security and privacy plans as interlocking system plans.
5. **Calendar each authorization backward from its expiry.** Run a readiness review against NIST SP 800-53A procedures and keep a continuous monitoring calendar, so no ATO date arrives with only an extension request in motion.

This work doesn't grant authorizations, approve PIAs, or replace the independent assessment, and it doesn't guarantee an outcome.

WHAT "FIXED" LOOKS LIKE

GAO has published closure evidence for several recommendations in this report, as of its status notes.

REC	SUBJECT	GAO STATUS	CLOSURE EVIDENCE
5	ASPR cooperative agreement platform PIA	Closed, verified January 2026	PIA approved by the Senior Agency Official for Privacy, August 2025
8	EMR ATO	Closed, verified January 2026	GAO verified; details not shown in its note
11	FDA PIAs	Closed, verified May 2025	PIAs for four of seven systems; analyses found the other three did not require one

The FDA closure is the precedent for CDC: GAO accepted written analyses showing three systems needed no PIA.

For the open CDC recommendations, these are targets:

- Every CDC pandemic system that holds PII has a current PIA or a written determination that none is required.
- Each categorization memo carries a recorded privacy-official approval.
- Every ATO has an expiry date on a calendar owned by a named person.

STATUS CHECK

MIXED Of the 14 recommendations, GAO lists 8 closed and 6 open as of its latest notes. CDC recs 9 and 10 were open as of GAO's December 2025 update, with no supporting evidence provided at that point. Recs 1 through 4, on a department-wide system list, duplication, funding, and staffing, were also open then.

TEAMING FIT

NAICS	541512, 541519
AVALON'S SUB ROLE	Privacy threshold analysis and PIA support artifacts, FIPS 199 categorization memos routed for privacy-official review, SSP and control-inheritance documentation, and a readiness review ahead of the independent assessment, under the prime's A&A task
SMALL-BUSINESS STATUS	Small business; HUBZone (in progress)
LIKELY VEHICLES	GSA MAS (SIN 54151HACS Highly Adaptive Cybersecurity Services); GSA MAS (SIN 54151S IT Professional Services); GSA Alliant 3

If HHS or CDC authorization and privacy documentation is in your capture plan, Avalon teams as the sub that builds the PIA register, the categorization memos, and the assessment-ready package behind each system's ATO.

BRANDON IRELAND, FOUNDER · CONTACT@AVALONTECHSERVICES.COM · AVALONTECHSERVICES.COM

This brief analyzes publicly released oversight reports. It does not describe work Avalon performed for any agency named.