Palantir

Checkpoints

September 2025

PALANTIR.COM

ALCOA+, 21 CFR Part 11, and GxP Regulatory Standards

ALCOA+ & GXP REGULATORY STANDARDS

Palantir empowers organizations to make data-driven decisions with confidence, security, and integrity. Across our platforms and products, we prioritize the highest standards for data management, ensuring that data is not only accessible but also reliable and trustworthy throughout its lifecycle. Our solutions are designed with the ALCOA+ principles (Attributable, Legible, Contemporaneous, Original, and Accurate) at their core, providing robust controls for attributing actions, maintaining legibility, ensuring contemporaneous data capture, and preserving the originality and accuracy of records. Features such as granular audit trails, secure access controls, and comprehensive data lineage tools enable customers to demonstrate compliance with industry regulations and internal policies alike. By embedding these capabilities into our technology, Palantir delivers a strong foundation for organizations seeking to uphold the strictest standards of data integrity.

In highly regulated industries, maintaining uncompromising data integrity is essential — not just for operational excellence, but also for meeting the rigorous standards set by regulations like the Food and Drug Administration's (FDA's) Title 21 Code of Federal Regulations (CFR) Part 11regarding Electronic Records and Electronic Signatures. The ALCOA+ principles provide a comprehensive framework to ensure the reliability and trustworthiness of electronic records and signatures. Palantir Foundry, enhanced by our Checkpoints product, brings these principles to life by embedding configurable, auditable stop-checks directly into critical workflows. By integrating Checkpoints across Palantir's platforms, organizations can enforce controlled actions, capture secure and tamper-evident records, and demonstrate end-to-end traceability — empowering customers to confidently achieve and sustain regulatory compliance.

21 CFR PART 11

Comparing the Checkpoints application, in tandem with the baseline compliances maintained by Palantir's Foundry, here are just a few examples of how 21 CFR Part 11 compliance is systematically maintained:

- Of Subpart B - Electronic Records:
    - Regarding § 11.50 Signature manifestation:
        - Checkpoints records the full printed name in relation to the user executing said action, along with the date and time of execution, including the meaning and/or justification of said action, in relation to the e-signature retained. This requirement is equally supported by the Checkpoints Review interface, in an easy-to-navigate, human-readable presentation.
    - Regarding § 11.70 Signature/record linking:
        - Checkpoints supports a direct connection to the implicated resource (i.e., electronic record) to which the e-signature is related. In tandem, the resource's native RID is linked to the checkpoint, and the checkpoint action itself creates a Checkpoint Interaction ID that is natively stored within Foundry's Audit Logging function, ensuring the signature cannot be transferred, copied, or otherwise falsified.
- Of Subpart C - Electronic Signatures:
    - Regarding § 11.100 General requirements:
        - Each Checkpoint signature is unique to one individual and cannot be reused or reassigned.
        - Checkpoint configurations can support unique verbiage or consents to accompany each checkpoint action to associate the e-signature occurrence with a legally binding equivalent of the user's handwritten signature.
    - Regarding § 11.200 Electronic signature components and controls:
        - Foundry system controls ensure that, at a minimum, all requirements for e-signatures not based on biometrics are natively controlled for, including, but not limited to: distinct identification components for execution of signatures, controls for assurance of signatures based on executed users, and controls for contemporaneous signature execution.

This list of examples represents only a portion of the full 21 CFR Part 11 compliance capabilities that Checkpoints can support.

Overall, Checkpoints helps address on-going discomfort when synthesizing data of such a robust nature across multiple tooling applications: How do you ensure and manage the integrity and governance of the data accessed and relied upon by multiple users at any given point in time? Palantir's Foundry, utilizing the Checkpoints application in tandem with native controls such as Audit Logging, provides a means to control data integrity and governance across the multi-tooling offerings for a multitude of users. Palantir's systems are capable of processing and operating in highly sensitive environments where these controls are of paramount importance. Below, several use cases explore the usage of Checkpoints, demonstrating its configurable functionality in real-world operational workflows.

WITHIN THE PHARMACEUTICAL SITE SELECTION PROCESS

Site selection in the life science sector refers to the process of identifying and evaluating potential locations — such as hospitals, clinics, or research centers — to conduct clinical trials or research studies. This involves assessing factors like patient population, facility capabilities, regulatory compliance (including Good Clinical Practices), and previous performance to ensure optimal trial execution and data quality. Some examples of control points which may require e-signatures to maintain compliance standards include the following:

- **Site Feasibility Assessment Approval and or Site Selection Decision:**
    - The process by which approval is provided for completed site feasibility assessments, or a formal sign-off on the selection of a clinical site, may require e-signature controls to track the critical approval flow of said process, before proceeding with any regulated workflows.
- **Confidentiality Agreements (CDAs) & Conflict of Interest (COI) Declarations:**
    - Legally binding documentation such as the execution of confidentiality, non-disclosure, and COI disclosures and acknowledgments between sponsor and site, or investigator and staff, may require an e-signature compliant procedure to protect proprietary information before sharing trial details.
- **Investigator/Staff Training Records & Other Quality Control records**
    - Acknowledgments of required protocol, or other Good Clinical Practice (GCP)-implicated documentation may require an e-signature process to maintain minimum regulatory expectations including traceability and auditability.

WITHIN THE CLINICAL DATA TRIAL HARMONIZATION PROCESS

Clinical trial data harmonization involves standardizing and integrating data from multiple studies, often conducted at different sites or using varying protocols, to ensure consistency and comparability. This process enables researchers to combine datasets more effectively for meta-analyses, regulatory submissions, and broader scientific insights. Some examples of control points that may require e-signatures to maintain compliance standards include the following:

- **Data Mapping Approvals**
    - Approval of source-to-target data mapping specifications before harmonization begins may require an e-signature to validate the individual's authorization before moving forward with the use of the relevant data.
- **Data Release/Lock**
    - Authorization to release or lock harmonized data for downstream analysis or regulatory submission may require an e-signature to verify the individual and the rationale for performing the sensitive action.
- **Issue Resolution**
    - Approval of resolutions to significant data discrepancies, abnormalities, or issues identified during harmonization may require an e-signature process to track the specific corrective action performed, inclusive of rationale.

WITHIN REAL WORLD EVIDENCE ANALYSIS PROCESS

Real World Evidence (RWE) analysis involves examining data collected from real-world settings, such as electronic health records, insurance claims, and patient registries, rather than controlled clinical trials. This analysis helps assess the effectiveness, safety, and value of medical interventions in broader, more diverse patient populations, supporting regulatory decisions and healthcare policy. Some examples of control points that may require e-signatures to maintain compliance standards include the following:

- **Protocol Analysis Plan Approval**
    - Final approvals of the RWE study protocol or statistical analysis plan (SAP), may require a compliant e-signature process to ensure that the objectives, methods, and endpoints are formally reviewed and authorized. This signature type may also be extended to end report results, inclusive of findings, applicable for controlled dissemination.
- **Data Access, Sharing, or Disclosure Authorization**
    - Approvals related to internally accessing or externally providing sensitive real-world data sources, whether with regulators, partners, or publications, may require an e-signature to control and track the sharing of controlled data.
- **Data Extraction/ Transformation Approval**
    - Sign-offs on data extraction and transformation logic (e.g., ETL scripts) may require an e-signature to control and confirm that data processing steps are validated and maintain traceability.

While the above examples are not exhaustive, and Checkpoints may be integrated anywhere within an action-driven process tied to Foundry, Checkpoints can be uniquely configured to support the organization's specified use cases. Palantir is focused on building software platforms that not only solve for current global regulatory expectations, but that also stay at the cutting edge of new and ever-growing standards.