MEDIDATA | WHITE PAPER

Safeguarding Personal Data: myMedidata's Approach to Protecting Personally Identifiable Information (PII)

Table of Contents

Introduction

myMedidata offers a comprehensive suite of services designed to support Patients participating in clinical studies and pre- and post-trial engagement through myMedidata Registries. With a myMedidata account, Patients create and own lifelong access to the platform, enabling participation in clinical studies and registries while also serving as a central hub where Patients have indefinite access to their information and can leverage Patient Cloud services for all clinical trial activities. The use of myMedidata aligns with the growing emphasis on patient-centric drug development and the decentralization of clinical trials, as it empowers Patients and keeps them closely connected and engaged with all their studies and registries.

Setting up a myMedidata account closely mirrors the typical process for setting up any online account requiring information, like providing an email address and creating a password. Furthermore, myMedidata's lifelong account, accessible via the web and mobile app, is comparable to the commonplace accounts that users access across many industries, such as education, healthcare, finance, and social media and online communities. Importantly, Patients create and maintain their myMedidata accounts independently of any specific clinical trial, ensuring continuous access and control over their account regardless of their trial participation. myMedidata also offers Patients and Caregivers the opportunity to provide optional additional information that is used to create a more personalized experience within the platform.

Patients and Caregivers can access myMedidata and complete tasks using any web-enabled device or through dedicated iOS and Android applications. An important aspect of myMedidata is the collection of personally identifiable information (PII) that includes identifiable and demographic data. This PII is used to engage and support Patients throughout their entire journey—before, during, and after—in both studies and registries, enhancing myMedidata's ability to create a highly personalized experience that leads to greater patient satisfaction and better clinical studies. An important differentiator for myMedidata versus other clinical systems, is that the Patient or Caregiver is the manager of their own account, which is granted to them independently of a sponsor's study or any other pre- or post- trial engagements. This ensures that the Patient or Caregiver has control of their account via access controls that are compliant with 21 CFR part 11, Annex 11 and other global digital and electronic signature regulations.

While Medidata recognizes that sharing PII may cause concern for some individuals, this paper outlines the benefits for Patients and describes the security measures myMedidata uses to protect PII. Additionally, it explains how these measures adhere to ALCOA+ principles, ensuring the reliability and traceability of clinical trial data.

Benefits for Patients

myMedidata offers Patients a single, secure, lifelong account that enables them to participate in clinical studies and registries on the platform. This keeps Patients closely connected and engaged with all of their studies and registries, aligning with the growing emphasis on patient-centric drug development, considered to be "a systematic approach to help ensure that Patients' experiences, perspectives, needs, and priorities are captured and meaningfully incorporated into drug development and evaluation."[1]

By having a myMedidata account, Patients and Caregivers can learn about clinical trials, provide their consent and re-consent remotely, participate in LIVE video visits, setup and receive payments, and share patient reported clinical outcomes, eDiary data and other information all through myMedidata.

As previously referenced, myMedidata accounts offer Patients support and convenience through a single account with features such as **(Figure 1)**:

- myMedidata eCOA
- myMedidata eConsent
- myMedidata LIVE video visits
- myMedidata Registries
- Patient Payments
- Direct-to-Patient shipments

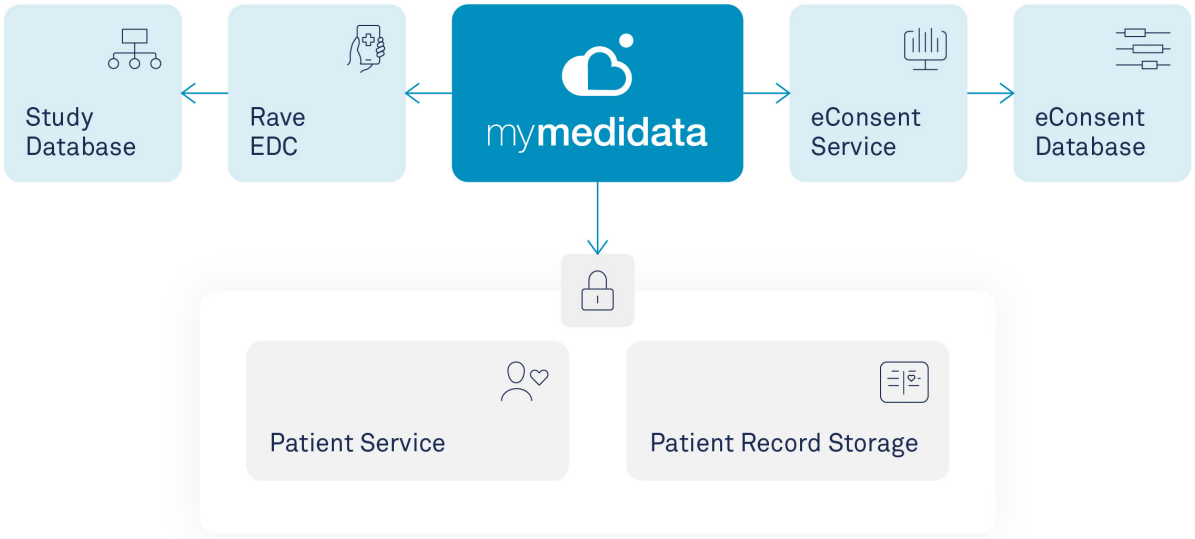


Figure 1: myMedidata integrates Medidata's eCOA and eConsent capabilities while also enabling LIVE video visits. myMedidata allows Patients to easily and securely complete forms, participate in video visits with their study team, receive reminders and notifications for study-related tasks, and access their results, using any device with an internet connection.

In addition to these features, myMedidata accounts can facilitate continuity of care during critical transitions between clinical research and clinical treatment. Poorly managed care transitions can result in adverse events, higher hospital readmission rates, and increased costs.[2] By empowering Patients with greater control, efficiency, and autonomy before, during, and after trial participation, lifelong access to myMedidata addresses a significant gap in the patient care continuum, particularly during challenging transitions between research and medical care or between registries and studies.

How myMedidata Uses PII

As with any personalized electronic system, some basic PII is essential for creating myMedidata accounts and supporting system workflows that keep Patients and their support networks engaged. For example, PII enables clinicians to better understand their Patients, assists with tasks such as countersigning, and helps identify when Patients' trial activities are supported by Caregivers. PII also ensures compliance with country-specific study requirements and regulations for services like myMedidata Web or myMedidata apps, while facilitating patient notifications, reminders, and reimbursements. Account security is a priority, and Patients can reset their passwords to maintain the integrity of their accounts.

Patients can choose to provide additional, optional PII to enhance their study experience. Instead of referring to Patients as a "subject number", preferred names are provided via a myMedidata account, allowing site personnel to recognize Patients as individuals and to make them feel valued. The optional PII also simplifies the experience for Caregivers that are managing multiple Patients by allowing them to easily identify individuals during form completion and other tasks.

How myMedidata PII Is Stored

myMedidata uses the latest Advanced Encryption Standard 256 (AES-256) algorithm during collection, transmission, and when storing both PII and PHI. Additionally, the system employs Transport Layer Security (TLS) v.1.2 to encrypt data while in transit between the collection device and the cloud based server. This allows collection devices to establish a publicly accessible connection with servers, while ensuring that only the device and server can decrypt and view transmitted information.

myMedidata centralizes PII storage for all Patients in a single, secure private cloud location rather than maintaining separate stores for each individual. This "walled garden" approach isolates PII with controlled links to clinical data, ensuring robust protection even when the information is used to support study and registry objectives.

Beyond PII, myMedidata accounts can function as secure repositories for Patients' health information. This centralized storage allows Patients to conveniently access their medical information through myMedidata's web portal and mobile applications, offering a single, user-friendly point of access that is especially beneficial during care and/or study transitions.

Who Can Access PII?

PII collected during account registration receives the same high-level protection as Medidata's clinical study data clients and is stored in Medidata's Patient Service database which is technically and administratively separate from any clinical study data.

Only users with specific PII-approved roles and secure credentials can view PII within the myMedidata and Patient Cloud Registration interfaces, and this information is not permanently stored outside the Patient Service database. Access to the Patient Service database is tightly controlled under our Covered Data Access Policy (POL-InfoSec-002-00), with only authorized service delivery team members permitted direct access for maintenance purposes. Sponsors do not have access to PII through iMedidata at any time.[3]

For production support, such as investigating errors, Medidata follows data access policies that only grant access to specific users for a period of time. Data access and duration are only approved by the Medidata Privacy Office. Internal use of Patient Service data is tightly controlled, with access restricted to specific uses that must be authorized at the application-level. This data is not available for general distribution or access.

Privacy by Design

An important concept of several Global Data Privacy Regulations in recent years is the expectation that organizations like Medidata will employ a proactive approach to protecting user privacy by embedding privacy considerations into the design and operation of systems, technologies, and business practices with the goal of anticipating and preventing privacy risks before they occur, rather than responding to breaches after the fact.

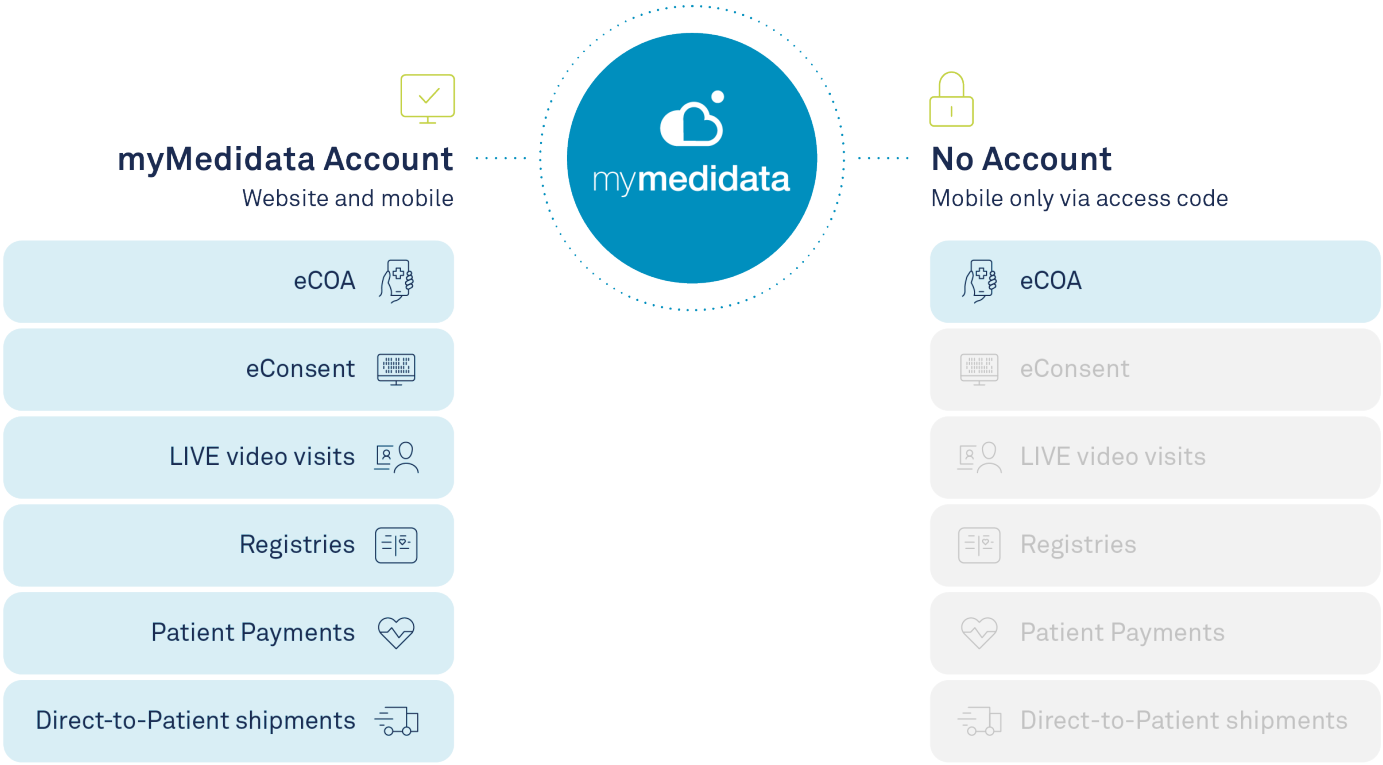
Medidata follows Privacy by Design principles and maintains detailed, formally documented inventories of applications and data across the entire Medidata Unified Platform. These inventories, created by product teams as part of the privacy by design process, outline the sources and locations of PII. Each business area uses a standardized template to specify the types of data collected, associated privacy risks, and the controls put in place to mitigate these risks.

The privacy by design process involves product owners evaluating projects that introduce new processes or modify existing ones involving Patients' personal information. These evaluations examine the impact on personal data and related controls. Medidata's Privacy Office (MPO) then assesses any risks associated with changes to PII processing within the Unified Platform. When control gaps are identified, they are documented, and corrective action plans are developed and executed to address these gaps.

Medidata maintains a ready state of Trust and Transparency through our Unified Protection Strategy to help our clients, partners, Patients and their Caregivers have confidence in how their data is collected, where it is managed, how long it is kept for, and what the purposes are of collecting the data. The core principles of our Unified Protection Strategy can be viewed online at https://www.medidata.com/en/trust-and-transparency/

Navigating PII Restrictions

myMedidata has been designed for global use and to navigate restrictions, such as regions where PII collection is prohibited. In this case, Medidata provides an alternative participation method for Patients in those regions, allowing them to engage in eCOA-only studies pseudonymously using the myMedidata iOS or Android mobile applications. This pseudonymous participation requires only an activation code for Patients to join a study, ensuring compliance with local regulations while still enabling patient involvement in clinical research. However, these Patients participating pseudonymously cannot join registries or use eConsent, LIVE video visits, Patient Payments, and other functionalities due to the collection of PII required for execution of the respective task, like a signature for eConsent. The inclusion of a country or region with restrictions that require participation using an activation code does not impact Patients from non-restricted regions on the same trial from participating with, and benefiting from, the full benefits of a myMedidata account.



About Global Data Privacy Regulations

In compliance with global privacy laws, core privacy principles such as data minimization, transparency, purpose limitation, security and accuracy are at the core of Medidata's privacy practices. The myMedidata Privacy Policy and Terms of Use presented to all users upon creating a myMedidata account outlines our privacy practices, including explanation of data subject rights available to a study participant in relation to their myMedidata account. The identifiers collected in myMedidata for the creation of user accounts are reasonably necessary and proportionate for Medidata to provide and maintain its services.

As the global regulatory landscape continues to evolve, there are certain jurisdictions where the collection of direct identifiers and pseudonymized clinical trial data may require additional steps to comply with local requirements. In France, for example, Commission Nationale Informatique & Libertes (CNIL) authorization may be required as Medidata's collection of the direct identifiers and pseudonymized clinical trial data potentially deviates from the MR-001 reference methodology.

Clients are advised to consult their own counsel for any requirements applicable to their specific study protocols; however, where clients opt to pursue any type of pre-authorization, Medidata provides the necessary support through our privacy assistance materials and assistance with completion of questionnaires.

Good Clinical Practice Discussion

The International Council for Harmonisation (ICH) E6 Good Clinical Practice (GCP) guidelines, including both the current "R2" and the newer draft "R3" versions, address patient privacy and confidentiality.

The privacy and confidentiality of patient data are foundational principles of GCP:

> ***The confidentiality of records that could identify subjects should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirement(s).***[4]

Furthermore, *confidentiality* is defined by the guidelines in the following way:

> ***Confidentiality: Prevention of disclosure, to other than authorized individuals, of a sponsor's proprietary information or of a subject's identity.***[5]

Looking ahead to the anticipated release of ICH GCP R3, the newest GCP draft[6] prescribes the following:

> ***The investigator/institution should implement appropriate measures to protect the privacy and confidentiality of personal information of trial participants in accordance with applicable regulatory requirements on personal data protection. Data reported to the sponsor should be identified by an unambiguous participant code that can be traced back to the identity of the participant by the investigator/institution.***[7]
>
> ***The sponsor should implement appropriate measures to protect the privacy and confidentiality of personal information of trial participants, in accordance with applicable regulatory requirements on personal data protection.***[8]

The GCP guidelines provide clear guidance on patient protections concerning confidentiality and privacy, which are governed by applicable data protection rules. However, these privacy and confidentiality rights are not absolute as they are subject to a balancing act that takes into consideration the principles of GCP and the privacy regulations relevant to the specific regions where clinical trials are being conducted.

While investigators must be able to identify and communicate with Patients, sponsors have limited rights to access PII for the purposes of auditing and monitoring. myMedidata's confidentiality controls are tailored to accommodate these differing needs, allowing investigators and sponsors to conduct their respective activities in compliance with GCP expectations. According to ICH GCP R2 section 4.8.10(n), monitors, auditors, IRB/IEC, and regulatory authorities may be granted direct access to subjects' original medical records to verify clinical trial procedures and data, without violating subject confidentiality, to the extent permitted by applicable laws and regulations.[9]

Data Integrity in Clinical Trials

The concept of *data integrity* in GCP is rooted in the ALCOA+ principles for records and reports, which are fundamental to ensuring the reliability and traceability of clinical trial data. ALCOA+ includes the following elements:

- Attributable
- Legible
- Contemporaneous
- Original
- Accurate
- Complete

Focusing on the first element, *attributable* means that data can be traced back to a specific individual. In other words "It should be obvious who documented or did what—it should be traceable to a person, date, and subject visit." This principle applies to all clinical data, regardless of who originates it, including Patients and their Caregivers. As clinical trials become increasingly decentralized, *attributability* becomes even more important to ensure that patient-shared data—such as patient-reported outcomes and sensor data—are properly attributed to Patients.

In traditional clinical trials, investigators and/or site support staff meet Patients in person, screen them, collect their contact information for correspondence, and use various tools to achieve these tasks. Investigators may also serve as gateways to electronic research tools that will be used by Patients. For instance, with myMedidata electronic patient-reported outcomes (ePROs), research sites create patient accounts and invite Patients to register using their email addresses.

Patients then register their accounts with additional personal information, serving as an attributability control. This process ensures that Patients can use their accounts and participate in the trial. Many other regulated industries use PII to validate accounts through multi-factor authentication and for troubleshooting purposes. When properly specified, managed, and protected, the use of PII enhances adherence to ALCOA+ principles.

Summary

myMedidata provides a comprehensive suite of services designed to support Patients participating in clinical studies and registries. Through their account, Patients gain lifelong access to this secure platform, which facilitates trial activities such as re-consenting for studies, receiving reimbursements, and participating in LIVE video visits from the comfort of their home.

myMedidata collects PII to enhance the patient experience at every stage of their journey. Medidata safeguards this information with advanced encryption standards and centralized storage, with strict controls on who can access this data. Adherence to GCP guidelines maintains patient privacy and confidentiality, and following ALCOA+ principles ensures the data's reliability and traceability.

References

1 FDA Patient-Focused Drug Development Guidance Series for Enhancing the Incorporation of the Patient's Voice in Medical Product Development and Regulatory Decision Making. Available at: https://www.fda.gov/drugs/development-approval-process-drugs/fda-patient-focused-drug-development-guidance-series-enhancing-incorporation-Patients-voice-medical

2 Rotenstein, L., Melia, C., Samal, L., Pollack, S., Yu, N., Cunningham, R., & Price, C. (2022). Development of a Primary Care Transitions Clinic in an Academic Medical Center. Journal of general internal medicine, 37(3), 582–589

3 iMedidata is a hosted clinical trial portal and user rights administration platform, which delivers a front-end for an enhanced user experience for all Medidata applications.

4 International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH). (2016). "Integrated Addendum to ICH E6(R1): Guideline for Good Clinical Practice E6(E2)." https://database.ich.org/sites/default/files/E6_R2_Addendum.pdf

5 Id.

6 International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH). (2023). "ICH Harmonised Guideline: Good Clinical Practice (GCP) E6(R3)." https://database.ich.org/sites/default/files/ICH_E6%28R3%29_DraftGuideline_2023_0519.pdf

7 Id. at p. 20

8 Id. at p. 39

9 R2, supra note 1, section 4.8.10(n), p. 17: "the monitor(s), the auditor(s), the IRB/IEC, and the regulatory authority(ies) will be granted direct access to the subject's original medical records for verification of clinical trial procedures and/or data, without violating the confidentiality of the subject, to the extent permitted by the applicable laws and regulations."

10 See generally Question 5: www.fda.gov/files/drugs/published/Data-Integrity-and-Compliance-With-Current-Good-Manufacturing-Practice-Guidance-for-Industry.pdf

11 See University Hospitals "Clinical Research Good Documentation Practices." Available at: https://www.uhhospitals.org/-/media/Files/For-Clinicians/Research/alcoac-documentation.pdf