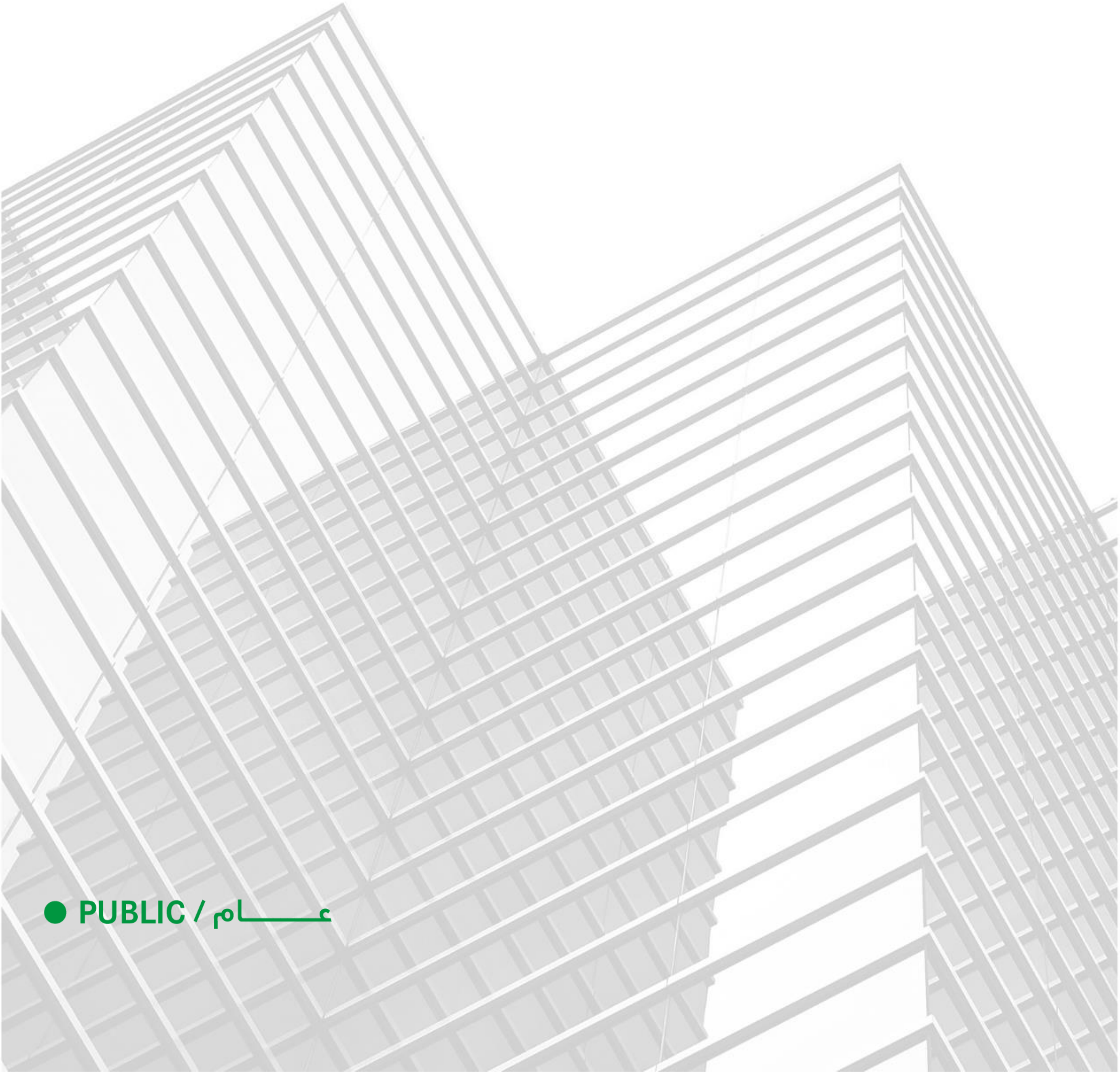
دائـــــرة الــصـــحـــة
DEPARTMENT OF HEALTH

POLICY FOR TRUSTED RESEARCH ENVIRONMENT (TRE)



● PUBLIC / عـــــــام

Document Title:	Policy for Trusted Research Environment (Tre)		
Document Ref. Number:	DoH/Policy/HLS/TRE/V1/2025	Version:	V1
New / Revised:	New		
Publication Date:	July 2025		
Effective Date:	September 2025		
Document Control:	DoH Strategy Sector		
Applies To:	- DoH Internal Sections - DoH licensed Healthcare Providers - DoH licensed Healthcare Professionals - Abu Dhabi Government Entities - Healthcare Researchers, Analysts, and Innovators - Research Funders - Data Custodians - Authorized Healthcare Facilities and Academic Institutes to conduct human subject's research. - Study Participants and Public - Any facility licensed and authorized by Department of Health for conducting research		
Owner:	Genome Division, Health Life Science Sector		
Revision Date:	July 2028		
Revision Period:	Three years from thor as deemed necessary		
Contact:	tre@doh.gov.ae		

1.Policy Purpose and Brief

1.1 BACKGROUND

The concept of Trusted Research Environments (TREs) has come to the forefront in an era marked by the exponential growth of digital data and the escalating concerns over data privacy and security. High-profile data breaches and increasing privacy concerns have highlighted the urgent need for stringent data governance mechanisms. At the same time, the potential of big data to drive significant breakthroughs in fields such as medicine, public health, and social sciences is more apparent than ever. This dual reality of risk and opportunity necessitates a balanced approach to data management—where the access to and use of sensitive information is meticulously controlled to prevent misuse while still enabling transformative societal advancements.

This policy should be comprehensively reviewed, comprehended, and executed alongside DoH regulations and guidelines concerning Healthcare Information, Data Governance, Data Quality, Data Catalogue, Meta Data Management, Cybersecurity, Human Subject Research, Patient Healthcare Data Privacy, Informed Consent, and pertinent UAE legislation on Data Protection and Safety.

1.2 PURPOSE

The purpose of this Policy is to establish requirements to ensure the integrity, transparency, and ethical conduct of research activities within the health sector of Abu Dhabi. The policy aims to create a secure and collaborative research environment, upholding integrity and ethical compliance to foster innovation and protect sensitive data, ensure confidentiality, and promote interdisciplinary collaboration.

1.3 OBJECTIVES

The objectives of this policy are multifaceted to ensure a secure, ethical, and collaborative research environment. These include:

1.3.1 Establish a secure and collaborative research environment.
1.3.2 Uphold standards of research integrity and ethical compliance to facilitate innovative and impactful research outcomes.
1.3.3 Protect sensitive data and ensure participant confidentiality.
1.3.4 Foster interdisciplinary collaboration and innovation.

2.Definitions and Abbreviations

No.	Term / Abbreviation	Definition
2.1	Access Control	Measures to ensure that access to assets is authorized and restricted based on business and security requirements.
2.2	Analyst	A specialist who examines and interprets data to provide insights and support decision-making within a particular area of expertise.
2.3	Application Programming Interface (API)	A communication protocol between different software elements.
2.4	Audit	A systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.
2.5	Authentication	Provision of assurance that a claimed characteristic of an entity is correct.
2.6	Availability	A property of being accessible and usable on demand by an authorized entity.

2.7 **Competence**

Ability to apply knowledge and skills to achieve intended results.

2.8 **Confidentiality**

Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

2.9 **Conflict of Interest**

A conflict of interest arises when an individual or organization has multiple, often competing interests—financial or otherwise—wherein serving one interest could potentially undermine or conflict with another. This situation typically occurs when actions or decisions made in their professional or official capacity may lead to personal gain or benefit, creating a potential bias or conflict in fulfilling their duties impartially.

2.10 **Certificate of Record and Destruction (CORD)**

A formal document issued at the closure of research activities in a TRE, certifying that all temporary working copies of datasets have been securely deleted or migrated to an approved archival location within the TRE, and clearly documenting any derivative datasets retained under new ethical approval or data-sharing protocols. It includes explicit confirmation of these actions, listing involved datasets, dates, methods, and responsible parties.

2.11 **Data Custodians**

The individual/unit responsible to execute data-related initiatives and decisions associated with data management domains from a technical aspect. Serves as subject matter experts in information management, specializing in data systems/applications.

2.12 **De-identification**

The process of removing or obscuring personal identifiers from data sets, in a manner that the individual to whom the data pertains can no longer be identified, whether directly or indirectly allowing data to be used in research while protecting privacy.

2.13 **Data Model**

A standardized representation of data assets, defining the attributes, and relationships between them to support data integration, consistency, and decision-making across the enterprise.

2.14 **Data Quality**

The overall condition of data based on attributes such as accuracy, completeness, consistency, validity, timeliness, and uniqueness.

2.15 **Dataset**

Collection or group of related data elements.

2.16 **Department of Health (DoH)**

The regulative body of the Healthcare Sector in the Emirate of Abu Dhabi, established based on law No .(10) of 2018.

2.17 **Encryption**

The process of converting information or data into a code format, especially to prevent unauthorized access and securing data by ensuring that only people with the correct key can decode and view the contents.

2.18 **Ethical Conduct**

Behavior that is consistent with the principles of ethical standards embraced by a particular profession or environment. It includes honesty, fairness, and integrity in professional practices.

2.19 **Innovator**

A researcher, who introduces new ideas, products, or methods, often with a focus on creativity and problem-solving, to drive positive change and progress in various fields or industries.

2.20 **Integrity**

A property of accuracy and completeness.

2.21 **Interoperability**

The ability of different information technology systems and software applications to access, exchange, integrate, and cooperatively use data in a coordinated manner, within and across organizational boundaries. It involves the seamless sharing of data among various systems, platforms, or components, ensuring that the data shared retains its meaning and does not lose its context or integrity.

2.22 **Metadata**

Structured information that describes, explains, or provides context about a dataset, making it easier to find, manage, and utilize the data. It includes details such as the source, format, creation date, author, and relevant keywords as well as any technical and administrative information necessary for effective data governance, access, and interpretation.

2.23 **Reliability**

A property of consistent intended behavior and results.

2.24 **Safe Data**

Research data that is securely stored, transmitted, and handled within the Trusted Research Environment to maintain confidentiality, integrity, and compliance with ethical and regulatory standards.

2.25 **Safe Output and Release**

Secure dissemination of research findings or data outputs from the Trusted Research Environment, ensuring confidentiality, integrity, and compliance with ethical and regulatory standards throughout the release process.

2.26	**Safe Personnel**	Certified and trained professionals responsible for upholding ethical and security standards while handling sensitive research data within the environment.
2.27	**Safe Research Projects**	Approved research projects for appropriate data access and justified public benefit and ethical considerations.
2.28	**Safe Return**	A secure retrieval or transfer of research data or materials from external sources back into the Trusted Research Environment, ensuring confidentiality, integrity, and compliance with ethical standards throughout the return process.
2.29	**Safe Systems and Processes**	Secure and sovereign technological infrastructure and protocols ensuring confidentiality and integrity of research data.
2.30	**Terms of Use**	A legal agreement that outlines the rules and guidelines that users must agree to and follow in order to use a service or software.
2.31	**Trusted Research Environment (TRE)**	A secure environment where researchers can safely store, analyze, and share sensitive data while adhering to strict ethical, legal, and regulatory standards.
2.32	**Validation and Verification Processes**	Processes that are used to ensure that a system, component, or system requirements meet their intended purpose and are correct, complete, adequate, and achievable.

3.Policy Content

3.1 BUILDING A SECURE FOUNDATION: ESTABLISHING GOVERNANCE

Establishing strong governance structures is fundamental to creating a secure environment for trusted research to ensure integrity, transparency, and compliance. Establishing governance mechanisms in line with the below requirements is vital to fostering accountability and ethical conduct, laying the foundation for a trusted research environment:

3.1.1 Establish a clear organizational structure for the TRE, delineating key roles and responsibilities, and internal and external dependencies, including the formation of a Governance Board, Data Stewardship Committee, and Institutional Review Board.

3.1.2 Ensure that leadership possesses comprehensive knowledge of data governance, ethics, and pertinent privacy laws with particular emphasis on the secure handling and irreversible de-identification of health-related data.

3.1.3 Develop comprehensive data governance policies encompassing data privacy, security, access, sharing and usage, aligning with relevant federal laws and DoH protocols, guidelines, and standards.

3.1.4 Establish and enforce policies ensuring the robust and irreversible de-identification of data, clearly defined consent procedures, legally binding data sharing agreements, and detailed breach notification protocols that prioritize the protection of re-identifiable information.

3.1.5 Allocate essential resources to support ongoing dialogues and transparency initiatives, as outlined in Section 3.2, and implement core principles detailed in Section 3.3 of this Policy.

3.1.6 Ensure that all personnel involved possess the required competence including information security due diligence for their authorized roles and that their performance is periodically assessed.

3.1.7 Integrate ethical considerations into all operations of the TRE, ensuring that data usage benefits society while safeguarding individual privacy at all stages.

3.1.8 Actively engage with stakeholders, including public and patient groups, researchers, healthcare providers, and funders, to cultivate trust and transparency.

3.1.9 Enforce stringent role based access controls based on the principle of least privilege, permitting only authorized individuals to access sensitive data with explicit, time bound authorization.

3.1.10 Implement multi-factor authentication, robust identity verification processes, and regular access reviews to uphold data security.

3.1.11 Implement stringent data security measure including encryption, data masking, and Differential Privacy

3.1.12 Establish full compliance with applicable DoH regulations on data sharing, import/export restriction, and national data sovereignty.

3.1.13 Establish quality management processes, encompassing document control, standard operating procedures (SOPs) management, and quality assurance audits.

3.1.14 Foster a culture of continuous improvement, soliciting feedback from stakeholders and adapting governance practices based on lessons learned and evolving best practices.

3.1.15 Conduct comprehensive periodic risk assessments for all data processing activities, explicitly identifying and mitigating risk of data leakage, re-identification, and addressing potential threats to data privacy and security.

3.1.16 Conduct classification of data where certain categories of sensitive data shall remain strictly restricted and shall never be shared, transferred, or exported under any circumstances.

3.1.17 Ensure ongoing compliance with legal and regulatory requirements, adjusting governance practices as needed to reflect changes in the legal landscape.

3.1.18 Develop and implement mandatory training programs for all TRE members, ensuring they comprehend their roles and responsibilities, data privacy laws and techniques to prevent inadvertent or intentional re-identification within the governance framework.

3.1.19 Adherence to data governance standards and protocols during the full life cycle of the TRE implementation.

3.1.20 The TRE program shall include detailed descriptions of roles for data/product owners, and outlining their responsibilities in defining TRE strategy, oversight platform development, reporting structure, membership criteria, escalation hierarchy, and operational metrics.

3.1.21 Promote awareness of data governance policies and ethical considerations among researchers and other stakeholders.

3.1.22 Implement monitoring and evaluation mechanisms to assess the effectiveness of governance policies and practices, with special focus on detecting unauthorized access attempts, potential data misuse, or re-identification vulnerabilities.

3.1.23 Regularly report on governance activities, compliance status, and any breaches or incidents to the Governance Board and relevant stakeholders.

3.1.24 Ensure transparency in governance processes, decision-making, and data use outcomes.

3.1.25 Engage with the public and patients through consultations, advisory groups, and clear communication regarding data usage and protection within the TRE.

3.2 FOSTERING TRUST: CONTINUOUS DIALOGUE AND TRANSPARENCY

Ongoing communication and transparency are essential for building trust in the research ecosystem. These objectives shall be achieved by:

3.2.1 Developing and maintaining more than one communication channel including but not limited to digital platforms, public forums, and direct outreach programs for engaging with the public, participants, patients, researchers, data custodians, funders, and relevant stakeholders.

3.2.2 Utilize plain language to articulate complex concepts, emphasizing the benefits and safeguards associated with data usage in TREs.

3.2.3 Periodically host workshops and forums with patients, public groups, researchers, and data custodians to collaboratively design TRE processes and address concerns.

3.2.4 Ensure comprehensive technical documentation on security designs, data protection measures, and governance structures is provided for independent review to verify compliance with standards and enhance transparency.

3.2.5 Facilitate assessments conducted by DoH, ensuring that records are accessible to offer an impartial evaluation of Trusted Research Environment (TRE) security and effectiveness.

3.2.6 Maintain a public log of data usage, approved research projects, and outputs from TREs to promote accountability.

3.2.7 Offer training for researchers and data custodians on data ethics, privacy protection, and technical aspects of TREs to enhance understanding and capability.

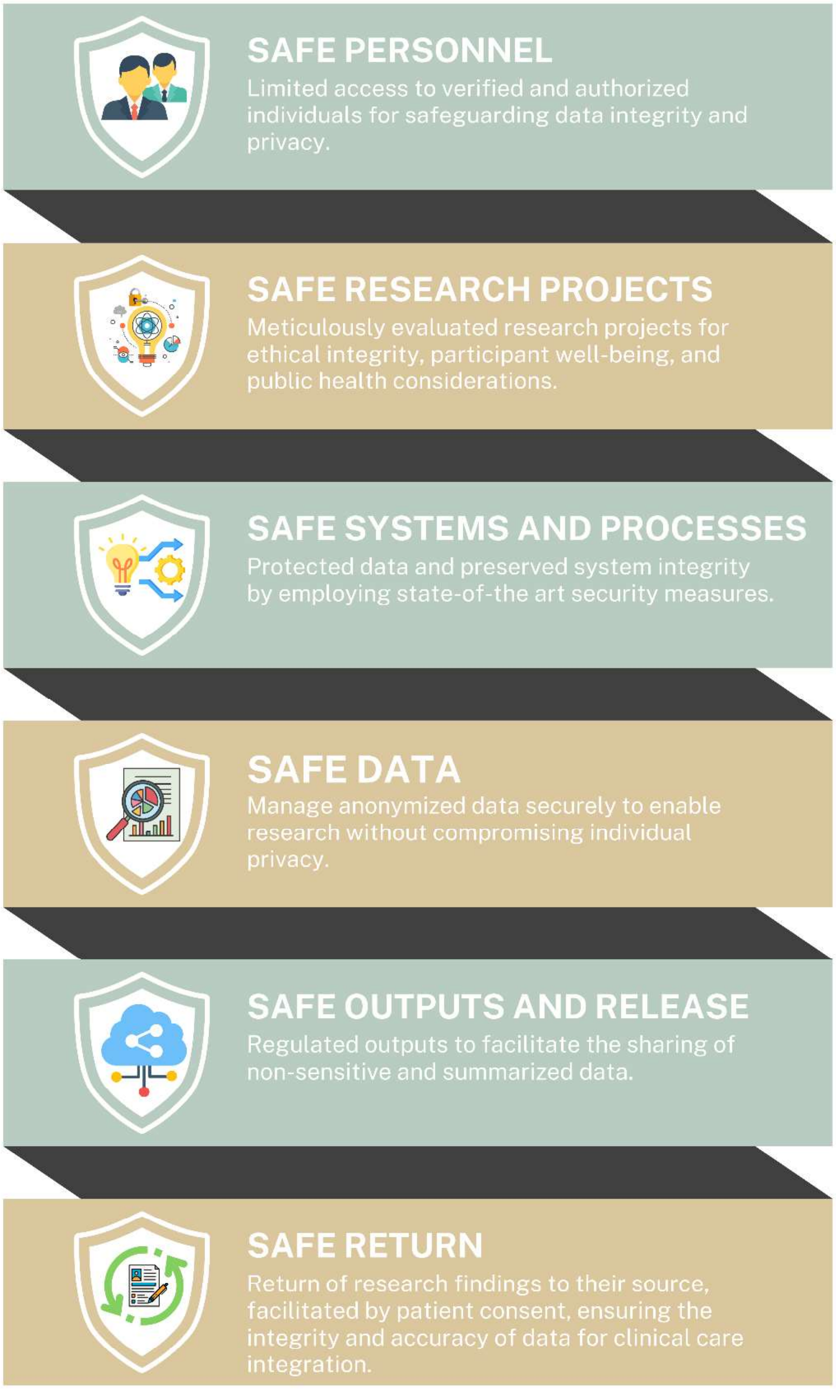
3.2.8 Develop targeted educational initiatives to inform the public and patients about the benefits of TREs for health research.

3.2.9 Design organizational policies and practices governing TREs to be adaptable, effectively responding to emerging technologies, evolving data protection standards, and stakeholder feedback.

3.2.10 Develop and communicate clear procedures for responding to data breaches or misuse, including immediate stakeholder engagement and transparent investigation processes.

3.3 CORE PRINCIPLES FOR TRUSTED RESEARCH ENVIRONMENT

TREs operate under core principles (Figure 1) ensuring integrity, security, and effectiveness in handling sensitive data. These principles support robust, ethically sound research by addressing personnel, project management, and technical systems, fostering public trust, and advancing healthcare.



SAFE PERSONNEL

Limited access to verified and authorized individuals for safeguarding data integrity and privacy.

SAFE RESEARCH PROJECTS

Meticulously evaluated research projects for ethical integrity, participant well-being, and public health considerations.

SAFE SYSTEMS AND PROCESSES

Protected data and preserved system integrity by employing state-of-the art security measures.

SAFE DATA

Manage anonymized data securely to enable research without compromising individual privacy.

SAFE OUTPUTS AND RELEASE

Regulated outputs to facilitate the sharing of non-sensitive and summarized data.

SAFE RETURN

Return of research findings to their source, facilitated by patient consent, ensuring the integrity and accuracy of data for clinical care integration.

Figure 1: Core Principles of Trusted Research Environment (Source: Conceptualized from UK Health Data Research Alliance)

3.4 OPTIMAL APPROACHES FOR IMPLEMENTATION

3.4.1 Safe Personnel

3.4.1.1 Access and Accreditation

3.4.1.1.1 Implement provisions to ensure that access to the TRE is granted solely to individuals with validated credentials who engage in projects that meet the established data access criteria. Eligible individuals include analysts and researchers from healthcare, academia, government, and other industries that offer valuable data science expertise.

3.4.1.1.2 Develop a rigorous certification process for individuals and engage in an accreditation process for organizations through an authorized accreditation body for identity and professional status verification, along with compulsory information governance training.

3.4.1.1.3 Establish criteria to accommodate individuals from diverse backgrounds, such as those with data science expertise from fields like social sciences, finance, or start-ups.

3.4.1.1.4 Ensure transparency regarding data access, backgrounds, and interests to uphold trust and address potential conflicts of interest, all while maintaining data security and trust.

3.4.1.1.5 Ensure access to the TRE is regulated by a robust authorization system. Only individuals with the requisite credentials and involvement in approved projects meeting data access requirements shall be granted entry.

3.4.1.2 Responsibility and Accountability

3.4.1.2.1 Organizations must ensure accountability for their employees' actions by ensuring compliance with organizational TRE policies, aligning with this Policy, and confirming the adherence of each individual.

3.4.1.2.2 Researchers must promptly inform the TRE of any changes in their institutional affiliations to ensure that their access privileges accurately reflect their current role and project.

3.4.1.3 Legal and Ethical Conduct

3.4.1.3.1 All users must sign legally binding terms of use agreements including non-disclosure agreements to ensure the integrity and security of the TRE. These agreements shall strictly prohibit:

3.4.1.3.1.1 Any attempts to re-identify individuals

3.4.1.3.1.2 Exploiting system vulnerabilities

3.4.1.3.1.3 Sharing login credentials

3.4.1.3.1.4 Using data for other purposes

3.4.1.3.1.5 Engaging in any activity that discloses the confidentiality, integrity, or availability of data, systems, or user accounts within the TRE.

3.4.1.3.1.6 Attempting to circumvent access to controls, encryption measures, or audit mechanisms implemented within the TRE.

3.4.1.3.1.7 Failing to report known or suspected security breaches, policy violations, or unauthorized disclosure within a reasonable time frame.

3.4.1.3.1.8 Retaining, duplicating, or exporting data outside the approved TRE infrastructure, unless explicitly authorized in writing by the data controller or custodian.

3.4.1.3.2 Implement processes to document and manage declarations of funding, sponsorship, commercial interests, and potential conflicts of interest to maintain trust and integrity in research activities.

3.4.1.4 Authentication and Monitoring

3.4.1.4.1 Establish robust procedures for verifying the identity of individuals and maintaining up-to-date records of their information governance training and role-relevant certifications.

3.4.1.4.2 Maintain detailed logs of user activities within the TRE and enhance transparency in data usage.

3.4.1.4.3 Implement authorization policies to regulate access based on the specific approvals granted to each individual.

3.4.1.4.4 Establish clear processes for revoking access to individuals who breach service terms, including the appeals process to uphold fairness and accountability.

3.4.2 Safe Research Projects

3.4.2.1 Project Justification

3.4.2.1.1 All research projects seeking access to TRE data must furnish a thorough project description outlining the project's objectives, methodology, anticipated public benefits, details of funders/sponsors, ethical approvals from relevant IRBs, and the duration of data access required.

3.4.2.1.2 Projects must substantiate potential public benefit and provide justification for data use to align with the objectives of the TRE and meet the expectations of data subjects.

3.4.2.2 Pre-application Support

3.4.2.2.1 Data Custodians are required to facilitate the pre-application process for potential applicants by providing summary statistics, limited query interfaces, or direct responses to specific data queries for informed decision-making prior to the submission of a complete application to the DoH.

3.4.2.2.2 Assist applicants in preparing their submissions effectively by providing detailed guidance on the data access request process, including prerequisites, timelines, and the decision-making framework.

3.4.2.3 Application and Approval Process

3.4.2.3.1 Data Custodians are required to develop a clear and proportionate data access request form to gather all pertinent project information. This form must prioritize transparency and simplicity, with clearly defined timeframes and requirements to ensure an efficient application procedure.

3.4.2.3.2 Applicants must be regularly informed about the status of their application, including any processing delays. A fair and transparent appeals process must be established for applicants whose requests are denied.

3.4.2.3.3 Data access requests must include meaningful involvement of patient and public representatives in the decision-making process, reflecting a commitment to inclusivity and transparency.

3.4.2.3.4 Maintain a publicly accessible register of approved projects, updated in real-time, to ensure transparency regarding data usage within the TRE. This register must include lay summaries of projects to make the information accessible to the general public.

3.4.3 Safe Systems and Processes

3.4.3.1 Security and Data Protection

3.4.3.1.1 TREs are required to deploy systems for securely storing data, ensuring encryption of individual-level data at rest.

3.4.3.1.2 Data shall be encrypted in use, at rest and in transit. Data encryption keys shall be stored separately in an on-premise HSM and must be under the exclusive control of DoH to prevent unauthorized access.

3.4.3.1.3 Data Masking to anonymize data and Differential Privacy to ensure no re-identification of data shall be implemented.

3.4.3.1.4 Strong Authentication and Authorization mechanism shall be in place including but not limited to Identity Access Management, Privilege Access Management, MFA, SSO etc.

3.4.3.1.5 Security designs and implementations must undergo independent audits by the DoH or authorized entities. Disclosure of audit results shall be governed by internal policy, subject to data protection and confidentiality constraints. The outcomes will be publicly disclosed at the discretion of the DoH to ensure transparency and foster trust.

3.4.3.1.6 Implement systems to securely monitor researcher activity within the TRE to ensure compliance with "Safe Research Projects" and prevent unauthorized data sharing, in accordance with "Safe Personnel" principles.

3.4.3.1.7 TRE providers must furnish assurance statements guaranteeing the conformity of their processes and systems to secure data processing as per DoH Information and Cyber Security regulations.

3.4.3.1.8 TRE providers must permit individuals to specify software, research code, reference data, and configurations for deployment within their Safe Systems. These specifications are subject to a review process and security assessment in a sandbox environment before deployment to ensure compliance with TRE policies and security standards.

3.4.3.2 Analytical Tools and Software

3.4.3.2.1 Offer a Safe research environment furnished with a comprehensive array of analytical tools. This environment must rigorously prevent data egress, ensuring data cannot be exported or copied to external systems.

3.4.3.2.2 Support the import of additional data, software, and algorithms as needed by researchers, subject to a review process to ensure security and compliance with organizational TRE policies and in alignment with this Policy.

3.4.3.2.3 Facilitate ongoing collaboration among project members by granting access to internationally recognized and authorized collaboration software within the Safes environment. This shall encompass tools for version control and shared document access, ensuring adherence to global standards.

3.4.3.3 Outsourcing and Cloud Computing Security

3.4.3.3.1 TREs utilizing public cloud services must be engineered to prevent data access by cloud service providers, ensuring data confidentiality and integrity and implementing "Safe Computing" within the Safe System.

3.4.3.3.2 Cloud Security shall align with all the Sovereign Controls established by UAE and the cloud security requirements from DoH.

3.4.3.3.3 Establish contractual arrangements with third-party providers alongside security design and engineering, to minimize the risk of data security breaches.

3.4.3.3.4 Data stored in the cloud must be encrypted at rest, in use and in transit with encryption key management infrastructure configured to ensure that only Data Custodians control the keys.

3.4.3.3.5 TREs must ensure transparency regarding cloud security measures by publishing comprehensive reports on cloud security design and implementation, detailing measures to prevent data access by cloud service providers and maintaining data confidentiality and integrity.

3.4.3.3.6 TREs must include the latest security technology stack as per requirement from DoH ICSO.

3.4.4 Safe Data

3.4.4.1 Data-sensitivity levels

3.4.4.1.1 For operational clarity, data held in the TRE are classified into four levels of sensitivity. The level assigned determines whether the data may leave the TRE and what controls apply. Export permissions are enforced through the Airlock process described in Section 3.4.5.

- **Level 0 – Aggregate / non-identifiable.** Summary statistics such

as GWAS results, allele frequencies and incidence counts. Export is permitted after statistical-disclosure control and Airlock approval.

- **Level 1 –** Variant-call files (gVCF / VCF) and phenotype tables that contain indirect identifiers only. Only Level 0 aggregates derived from these files may pass the Airlock.
- **Level 2 –** Alignment files (BAM / CRAM) remain inside the TRE, and only Level 0 aggregates may be exported after statistical-disclosure control and Airlock approval.
- **Level** 3 - Raw sequence feeds such as FASTQ and FAST5 are retained on secure in-house storage and are not released.

3.4.4.2 Data Accessibility and Usability

3.4.4.2.1 Data Custodians are required to share descriptive, semantic, and technical metadata for datasets in both human-readable and machine-readable formats to maximize the accessibility and usability of datasets within the TRE.

3.4.4.2.2 In Safe Data environments, prioritize the clarity and accessibility of data assets to reduce the need for extensive manipulation and analysis, especially when access is restricted to programmatic methods rather than a Virtual Desktop Infrastructure (VDI).

3.4.4.2.3 Ensure the effective, scalable, and consistent communication of dataset utility to enhance its usefulness and facilitate the assessment and comparison of datasets from diverse sources on a large scale.

3.4.4.2.4 Adopt common data models (i.e., OMOP and FHIR) to enable a collaborative research environment.

3.4.4.2.5 Implement provisions to delineate the essential metadata required for onboarding procedures that simplify the researcher's ability to search, organize, and filter datasets based on metadata rather than the raw data itself.

3.4.4.2.6 Data must adhere to the principles of Findability, Accessibility, Interoperability, and Reusability (FAIR) to ensure its optimal utilization and effectiveness.

3.4.4.3 **Privacy and Security**

3.4.4.3.1 Ensure organizational procedures provide comprehensive, easily understandable explanations for eliminating direct identifiers from source data assets prior to onboarding into the TRE. This involves employing uninformative pseudonyms to substitute direct identifiers, thereby safeguarding privacy while preserving the data's utility.

3.4.4.3.2 Standardize application programming interfaces (APIs) utilizing contemporary technical capabilities in computing standards.

3.4.4.3.3 Ensure that technical documentation required to engage with APIs is readily accessible to the public and provided free of charge.

3.4.4.3.4 Implement robust security measures for user authentication.

3.4.4.3.5 All data within the TRE must be encrypted both when stored and during transmission, serving as a compulsory security measure to safeguard against unauthorized access and potential breaches.

3.4.4.3.6 Provide data linkage services to support the merging of datasets within the TRE or with external data sources, contingent upon obtaining appropriate consents and permissions to expand research opportunities, allowing for more comprehensive and nuanced analyses.

3.4.4.3.7 Enforce data minimization practices commensurate with the sensitivity of the data and approved use cases.

3.4.4.3.8 Access controls must be aligned with minimum necessary use, ensuring privacy while facilitating appropriate data access.

3.4.4.4 **Project-Specific Data Spaces**

3.4.4.4.1 Establish the capacity to construct secure, project-specific workspaces within the safe environment to facilitate the integration of additional sensitive data or support research requiring isolated environments, thus ensuring both privacy and security.

3.4.4.4.2 Enable customized provisioning of data within project-specific spaces, tailored to research requirements and approved project scopes, to support hypothesis-generating research within the broader boundaries of project approval.

3.4.4.4.3 Ensure the preservation of data integrity and the enforcement of multi-tenant security and privacy within project-specific spaces. This involves limiting data access to authorized project members and implementing rigorous data protection measures.

3.4.4.4.4 Data provisioned for specific research shall be utilized solely for the scope of the research and shall not be utilized partly or wholly for any other requirements including another research even if approved.

3.4.4.4.5 Data provisioned and accessed shall not be shared further or outside the research team approved by the IRB.

3.4.5 Safe Import, Output and Release

3.4.5.1 Import Controls and Oversight

3.4.5.1.1 Establish a rigorous Airlock procedure for receiving datasets, software, container images and portable media destined for analysis inside the TRE.

3.4.5.1.2 Require every submission to carry a manifest detailing file type, size, data origin, checksum, and the approved research-project reference.

3.4.5.1.3 Run automated anti-malware, vulnerability, and checksum validation on all inbound files before human review.

3.4.5.1.4 Hold imports in a secure quarantine zone until the TRE Operations Team confirms the manifest, verifies that no direct identifiers or disallowed file types are present and authorizes release to the project workspace.

3.4.5.1.5 Assign authorized TRE Operations staff to supervise Airlock import requests, supported by the Data-Custodian oversight group.

3.4.5.1.6 Maintain clear documentation and training on approved file formats, container recipes, whitelists and security prerequisites to streamline the import process.

3.4.5.1.7 Log the manifest, reviewer ID, decision and date in the permanent audit record, and publish aggregated KPIs—such as median turnaround time and rejection rate.

3.4.5.2 Ownership of Research Output

3.4.5.2.1 Establish a legally binding agreement that defines the ownership and intellectual property rights and associated responsibilities. This includes, but is not restricted to, publications, datasets, software, and algorithms developed as integral components of the research process.

3.4.5.2.2 Promote the dissemination of research outputs within the confines of legal and ethical requirements.

3.4.5.2.3 Establish provisions to foster collaboration while honoring the intellectual property rights of all contributors.

3.4.5.2.4 Ensure that organizational policies are in accordance with the terms outlined in research funding agreements, which may specify particular requirements concerning the dissemination and utilization of research outputs.

3.4.5.3 Export Controls and Oversight

3.4.5.3.1 Data classified as Level 0 may be exported, subject to panel review and Airlock approval. Levels 1 through 2 remain within the TRE; only derivative Level 0 outputs generated from Levels 1–2 are eligible for export after statistical-disclosure control and Airlock approval (see level definitions in Section 3.4.4.1.1).

3.4.5.3.2 Prioritize minimizing data to only what is essential for reporting results, while accommodating cycles of rejection and revision as needed.

3.4.5.3.3 Designate personnel to supervise airlock export requests, with support from an oversight group.

3.4.5.3.4 Maintain comprehensive documentation and mandatory training programs on export options, summarization techniques, and minimization practices to streamline the review process.

3.4.5.3.5 Establish Key Performance Indicators (KPIs) on the speed and efficiency of the export review process within TREs.

3.4.5.3.6 Employ statistical disclosure control policies to assess data export requests, with documentation openly available detailing the criteria used for evaluation.

3.4.5.4 Archiving and Follow-up Access

3.4.5.4.1 Implement a mechanism for stably archiving datasets within the TRE that support publications but are restricted from export due to privacy concerns.

3.4.5.4.2 Assign externally visible identifiers to these datasets for reference in publications.

3.4.5.4.3 Establish provisions to enable temporary access to archived datasets for publication reviewers upon request, ensuring controlled access that upholds the integrity and validation of the research review process.

3.4.5.4.4 Offer services within the TRE to archive entire project workspaces for defined durations, facilitating the preservation of intermediate datasets and enabling follow-up or related research.

3.4.5.5 Project Close-out and Secure Destruction

3.4.5.5.1 Within 30 days of project expiry, the Principal Investigator must submit a Certificate of Return or Destruction (CORD) attesting that all temporary working copies stored in the project workspace have been deleted or migrated to an approved archival location within the TRE, and listing any derivative datasets retained under a new ethics or data-sharing protocol.

3.4.5.5.2 As part of the project off-boarding checklist, the TRE Operations Team disables user accounts, removes SSH keys and freezes export logs in accordance with UAE data-retention law.

3.4.5.5.3 Each quarter, the TRE Operations Team spot-checks at least ten percent of closed projects to verify the accuracy of submitted CORDs and reports the findings to the Data Custodian oversight group.

3.4.6 Safe Return

3.4.6.1 Ethical and Consent Management

3.4.6.1.1 Establish a comprehensive Health Information Systems (HIS) to track individual consents and withdrawals.

3.4.6.1.2 Ensure that the Safe Return of results to individuals or their healthcare providers is conducted exclusively for participants who have explicitly consented to this process.

3.4.6.1.3 Validate that Safe Return processes are backed by ethical approval from DoH, delineating the conditions under which research findings can be returned to the clinical setting for the benefit of individual patients.

3.4.6.1.4 Maintain detailed documentation of consent forms and ethical approvals to validate compliance and accountability, serving as a foundation for the ethical management of the Safe Return process.

3.4.6.2 Data Accuracy and Integrity

3.4.6.2.1 Data quality including accuracy, integrity, completeness and relevance shall be maintained as per the relevant standards and policies established by DoH from time to time.

3.4.6.2.2 Prioritize the overall data quality requirements of clinical data recording by clinicians, emphasizing the potential for research utilization to yield additional clinical insights.

4. Policy Roles and Responsibilities

The Department of Health (DoH)	• Overseeing this policy implementation to ensure a safe, secure, and trusted research environment within the Emirate of Abu Dhabi. • Review and approval of research protocols, especially involving human subjects or investigational products. • Conducting audits, inspections, and investigations to ensure compliance. • Engaging in public outreach to raise awareness about regulatory processes and research integrity. • Safeguarding the rights and well-being of research participants. • Fostering collaboration between stakeholders, healthcare providers, researchers, and industry stakeholders to promote research integrity.
DoH licensed Healthcare Professionals	• Ensuring adherence to research integrity requirements outlined in the policy. • Participating in research activities ethically and transparently. • Reporting any instances of research misconduct or breaches of integrity to the DoH. • Upholding confidentiality and privacy standards when handling research data or participant information. • Staying informed about the DoH requirements and best practices in research integrity. • Collaborating with all involved stakeholders to promote a culture of trust and transparency in research. • Engaging in ongoing education and training to enhance understanding of research ethics and compliance obligations.
Healthcare Analysts, Researchers, and Innovators	• Conducting research with integrity and transparency, aligning with this policy requirements. • Ensuring data accuracy, reliability, and security throughout the research process. • Incorporating patient perspectives and feedback into research design and implementation. • Collaborating with licensed healthcare professionals and the DoH to uphold ethical standards. • Engaging in interdisciplinary collaboration to ensure comprehensive and robust research outcomes. • Innovating responsibly, considering the potential impact on patient care and public health. • Participating in continuous education and training to stay updated on research best practices. • Reporting any research integrity breaches or misconduct to the DoH. • Contributing to a culture of trust and accountability within the healthcare research community. • Adhering to ethical practices when collecting, analyzing, and disseminating research data. • Leveraging analytical skills to interpret research findings accurately and ethically

Authorized Healthcare Facilities and Academic Institutes to Conduct Human Subjects Research	• Establishing and maintaining institutional policies and procedures in alignment with this Policy. • Providing resources and support for researchers to conduct human subjects research ethically and responsibly. • Ensuring compliance with the DoH requirements for the protection of human subjects. • Facilitating Institutional Review Board (IRB) or Ethics Committee review and approval processes for research protocols involving human subjects. • Training and educating researchers, analysts, innovators, and staff on ethical conduct and DoH compliance in human subject research. • Monitoring research activities to ensure adherence to approved protocols and ethical standards. • Investigating and addressing any instances of non-compliance or research misconduct promptly and appropriately. • Fostering a culture of ethical research conduct and transparency within the institution through communication and collaboration among stakeholders.
Data Custodians	• Safeguarding the confidentiality, integrity, and availability of research data in accordance with established DoH Standards and all Federal and local laws and Regulations of UAE. • Implementing appropriate data management practices to ensure data quality and reliability throughout the research lifecycle. • Facilitating access to research data for authorized purposes while protecting privacy and confidentiality. • Establishing data access and sharing agreements with researchers, analysts, and innovators to ensure compliance with legal and ethical requirements. • Providing support and guidance to researchers, analysts, and innovators on data handling, storage, and security best practices • Conduct regular internal audits and assessments to monitor compliance with data protection measures and address any vulnerabilities or breaches. • Collaborating with researchers, analysts, innovators, institutional leaders, and DoH to promote transparency and accountability in data custodianship. • Participating in ongoing training and professional development to stay informed about emerging trends and best practices in data management and security.
Study Participants and Public	• Stay informed about the purpose, risks, and benefits of research participation. • Provide informed consent before participating in any research study. • Advocate transparency and accountability in research practices. • Report any concerns or misconduct observed during research participation to DoH. • Engage in ongoing education about research ethics and the importance of trusted research environments.

Research Funders	• Setting clear expectations and requirements for research integrity and transparency in funding agreements and grant proposals. • Conducting due diligence to evaluate the credibility and reliability of research proposals and the integrity of researchers and research institutions. • Monitoring funded research projects to ensure compliance with agreed-upon standards and policies. • Providing guidance and resources to researchers on ethical conduct, data management, and reporting requirements. • Supporting initiatives to promote transparency and reproducibility in research findings. • Investigating claims of research misconduct or breaches of integrity and taking appropriate action, including funding suspension or termination if necessary. • Collaborating with research institutions, DoH, and other stakeholders to address systemic challenges and promote a culture of research integrity.

5. Policy Scope of Implementation

The policy applies to all research endeavors conducted within the healthcare domain, encompassing clinical trials, observational studies, health data analysis, and health services research. It extends to all healthcare professionals, researchers, analysts, innovators, clinicians, administrators, and staff involved in research activities within the organization.

This policy pertains to research involving human subjects, medical records, patient data, biological specimens, genome data, and other healthcare-related information. It applies across various healthcare settings, including hospitals, clinics, research centers, and academic institutions affiliated with healthcare delivery.

The policy implementation spans the entire research continuum, from protocol development and ethical review to data collection, analysis, and dissemination of research outcomes. It is designed to ensure the highest standards of research integrity, ethical conduct, patient safety, and data privacy within the healthcare research environment.

Through comprehensive training, education, and oversight mechanisms, the TRE Policy seeks to foster a culture of trust, collaboration, and excellence in healthcare research, ultimately contributing to improved patient care, healthcare outcomes, and public health.

6. Enforcement and Compliance

DoH may impose sanctions and penalties concerning any breach and /or non-compliance under this Policy in accordance with the disciplinary regulation of the healthcare sector.

A transparent reporting mechanism shall be established for individuals to report suspected violations or concerns regarding research integrity. Reports of non-compliance or research misconduct can be submitted anonymously to encourage open communication and accountability.

Reported incidents shall be promptly investigated by the Abu Dhabi Health Research and Technology Committee (ADHRTC) impartially and thoroughly, involving appropriate documentation, interviews, and evidence collection.

Depending on the severity of the violation, corrective measures may include warnings, sanctions, research protocol revisions, or termination of research funding or privileges.

7. Monitoring and Evaluation

The DoH shall ensure ongoing compliance, effectiveness, and improvement of policy implementation by:

- **Compliance Assessment:** Regular audits and assessments will be conducted to ensure adherence to the TRE Policy. Compliance reviews shall encompass various aspects of research activities, including but not limited to ethical standards, data management practices, and protocol adherence.
- **Data Analysis:** The collected data based on predefined indicators related to research integrity, ethical conduct, participant protection, and data security shall be analysed to identify trends, areas of non-compliance, and opportunities for improvement.
- **Feedback Mechanism and Continuous Improvement:** Inputs shall be gathered from stakeholders on policy implementation, informing ongoing refinement efforts. Continuous improvement initiatives shall be guided by monitoring findings, ensuring alignment with evolving standards and practices.
- **Performance Metrics:** KPIs shall be defined to track progress towards policy objectives and compliance.

8. Relevant Reference Documents

No.	Reference Date	Reference Name	Relation Explanation / Coding / Publication Links
1	December 2021	Alliance, U. H. D. R., & Nhsx. (2021b). Building Trusted Research Environments - Principles and Best Practices; Towards TRE ecosystems. In Zenodo (CERN European Organization for Nuclear Research).	https://doi.org/10.5281/zenodo.5767586
2	Retrieved April 25, 2024	The Complete Guide to Trusted Research Environments in 2023. (n.d.). Lifebit.	https://www.lifebit.ai/trusted-research-environment/complete-guide-2023
3	Retrieved April 29, 2024	Standard Architecture for Trusted Research Environments (SATRE). (n.d.). Satre Specification.	https://satre-specification.readthedocs.io/en/stable/index.html
4	May 2024	Abu Dhabi Healthcare Information and Cyber Security Standard V2.0	https://www.doh.gov.ae/-/media/78A323607B4C4ACAA58D0C9ACCFB3D59.ashx
5	June 2021	HDR UK – Recommendations for Data Standards in Health Data Research	https://www.hdruk.ac.uk/wp-content/uploads/2021/06/210622-Recommendations-for-Data-Standards-2021-Interim-Paper.pdf