Florida Cancer Research (CARES) Network & PAC3R Platform Data Access and Sharing Policy

Version 0.1
December 17, 2024

Table of Contents

Introduction 3
Objectives 3
Definitions of Abbreviations 4
Data Protection Classification 4
Public data 4
Research data governed by a consortium or research group 4
Confidential data governed by institutional policies 4
Regulated data governed by state of federal law 4
Access Controls 5
Role-Based Access Control (RBAC) 5
Roles 5
Administrator 5
Permissions 5
Member 5
Can be: a researcher, a data analyst 5
Permissions 5
Guest 6
Can be an external collaborator 6
Permissions 6
Data Security and Sharing Methods 6
Access Control 6
Data Sensitivity and Role-based Access Control (RBAC) 6
Data Ownership 6
Data Segmentation 6
Selective Data Sharing 6
Collaborative Data Sharing 6
Federated Data Sharing 7
Training 7
Audit Trail 7
Review and Revision 7
Incident Response 7
Document Version Control 8

Introduction

This Data Sharing and Access Policy document represents a foundational framework for the Bankhead-Coley Florida Cancer Research (FL CARES) Network Infrastructure to delineate the rules and procedures that govern data sharing, access, and management in the Platform for Accelerating Collaborative Computational Cancer Research (PAC3R, pronounced “pacer”). These policies support a secure, transparent, and compliant data ecosystem following the guidance of FAIR Principles in collaboration among the Florida CARES Network’s institutions, with a dynamic digital landscape essential for the automatic discovery of datasets and tools.

Objectives

The goal is to drive collaboration and innovation while safeguarding the privacy and security within PAC3R.

The data access and sharing policy described in this document is based on a culture of transparency, fortifying security measures, and ensuring compliance with pertinent regulations, as we increasingly rely on data to inform decision-making, drive innovation, and facilitate collaboration. The data shared, accessed, and managed within the Florida CARES Network organization or in external collaborations will:

- Promote responsible data management: Encourage the responsible use, access, and sharing of data to maintain its integrity, security, and accuracy.
- Ensure ethical handling of sensitive information: Establish best practice guidelines for handling sensitive, confidential, private data.
- Facilitate collaboration and information exchange: The Platform for Accelerating Collaborative Computational Cancer Research (PAC3R) provides a framework that enables seamless collaboration and information exchange, promoting innovation and knowledge sharing.
- Comply with relevant regulations and standards: Ensure alignment with applicable legal requirements, regulations, and standards, as well as data protection, privacy, and security.

Regular reviews and updates will ensure the access and classification level of access to data and tools according to the security measures, access controls, encryption, and audit trails implemented to the sensitivity level. We will implement training programs to ensure individual awareness of and adherence to data handling requirements within the PAC3R framework of policies.

Definitions of Abbreviations

FL CARES: Bankhead-Coley Florida Cancer Research Network Infrastructure.

PAC3R: Platform for Accelerating Collaborative Computational Cancer Research.
Pronounce “pacer”.

PII: Personally Identifiable Information.

API: Application Programming Interface.

RBAC: Role - Based Access Control.

PAC3R Access Control

FL CARES will follow data security best practices for access control into PAC3R, through secured sharing of data and for their specific roles.

Role-Based Access Control (RBAC)

Role-Based Access Control manages the predefined access to PAC3R in a structured and efficient way to control the functionalities and data per role via the application programming interface (API).

Roles

Administrator

Can be: site administrator account.

The PAC3R administrator has overall grants for user and dataset (endpoint) administration.

Permissions

- Has the authority to assign or revoke roles of users.
- Has the authority to assign or revoke access to datasets (endpoints).

Member (Contributor)/(Collaborator)

Can be: a researcher, a data analyst with an account.

The PAC3R member generates data. Conducts research and analyzes data. Integrates and analyzes data, derives insights, and generates reports.

Permissions

- Has access based on specific functions (expertise).
- Can analyze/interpret data per endpoints.
- Has access to specific datasets (endpoints, samples).
- Contributes to research projects.

Guest

Can be a collaborator with an account.

The PAC3R guest member can be anyone who has an account, can access tools to create signatures. The guest can download public data.

Permissions

- Limited, often read-only, access to specific datasets and research projects (publicly shared).
- Has access to specific data/tools based on the nature of the collaboration.

Data Protection Classification

FL CARES data classification for PAC3R is a critical aspect of ensuring responsible handling and protection of sensitive information for next-generation cancer sequencing and research. The classification categorizes the data based on sensitivity, criticality, and specificity of research impact. Cancer research discovery fosters collaboration and innovation toward safeguarding the privacy and security of patient data and genomic information. Regular reviews and updates shall be conducted to adapt these guidelines to changes in regulation, technological advances, and the evolution of cancer research. The data classification process takes into account the type of information, and the data lifecycle, from collection and storage to sharing and disposal.

Public data

Publicly accessible data that do not contain confidential, sensitive, or PII.

Research data governed by a consortium or research group

Data intended for internal use within PAC3R, which may include non-sensitive research data and aggregated statistics.

Confidential data governed by institutional policies

Critical data that require protection and access restrictions, governed by institutional agreements. For example: Patient data involving severe medical conditions, proprietary research findings, and any data subject to legal or confidentiality agreements.

Regulated data governed by state of federal law

Sensitive information such as personally identifiable information (PII) or information that could be used to identify individuals. For example: Patient medical records, genomic data, and any data that could lead to the identification of individuals.
Highly sensitive data that require strict access controls and additional security measures. For example: genetic information, clinical information, experimental results, and any data that pose a high risk if accessed by unauthorized individuals.

Data Security and Sharing Methods

Role-Based Access Control (RBAC) is a security approach that restricts access to authorized users based on their roles within each Organization and within the Bankhead-Coley Florida Cancer Research Network Infrastructure (FL CARES). RBAC is applied to manage functionalities, features, and data flow of PAC3R, with the necessary permissions for specific roles, to prevent unauthorized access.

Access Control

- Only administrators can modify system configurations.
- Only administrators can grant access to PAC3R.

Data Sensitivity and Role-based Access Control (RBAC)

- RBAC is integrated with data classification to ensure the safeguarding of sensitive data.

Data Ownership

- Datasets are unambiguously associated with an owner who has control over the data.
- Regarding the researcher who uploaded the data, either this researcher maintains the data, or the Institution maintains and has the ownership of the data.

Data Segmentation

- Datasets are segregated based on sensitivity and research project requirements.

Selective Data Sharing

- The act of choosing specific datasets or information to share with designated individuals or groups while retaining control over access to other data.

Collaborative Data Sharing

- Sharing data with the intention of fostering collaboration, typically between the data owner and external parties such as researchers, partners, or other organizations.
- Allows researchers to share specific datasets or findings within approved limits.
- Access must be requested and granted (temporarily) to specific datasets for collaborative purposes.

Federated Data Sharing

- A model where data are distributed across different locations or organizations, and access is granted in a coordinated and controlled manner.

Training

Training will be provided for users on the roles and associated responsibilities to ensure the understanding of the access scope.

Audit Trail

The FL CARES Network team and PAC3R development team will maintain an audit trail per role assignment, and will monitor compliance.

Review and Revision

The implementation of RBAC in PAC3R streamlines access management, ensures that individuals have access to only the necessary content for their roles, and enhances security and overall administration.

Incident Response

Regular reviews of this Data Access and Sharing Policy will incorporate feedback, address emerging challenges, and ensure alignment with evolving regulatory requirements. Clearly defined reporting mechanisms will adhere to the relevant obligations.

Document Version Control

Version	Sign Off	Comments
Version 0.0.10 March 28, 2024	C.Chung	Incorporated edits and comments.
Version 0.1 December 17, 2024	S. Schurer C. Obregon M. Pilarczyk D. Vidovic L. Rupprecht M. Sinclair V. Stathias C. Chung	Review of roles