Privacy Threat Modeling Genomic Workflows

Stuart Shapiro PhD, CIPP/US, CIPP/G

Principal
Nemo Jr Consulting

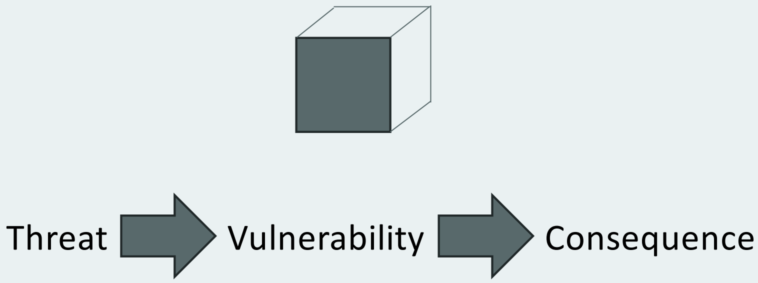
14 November 2025

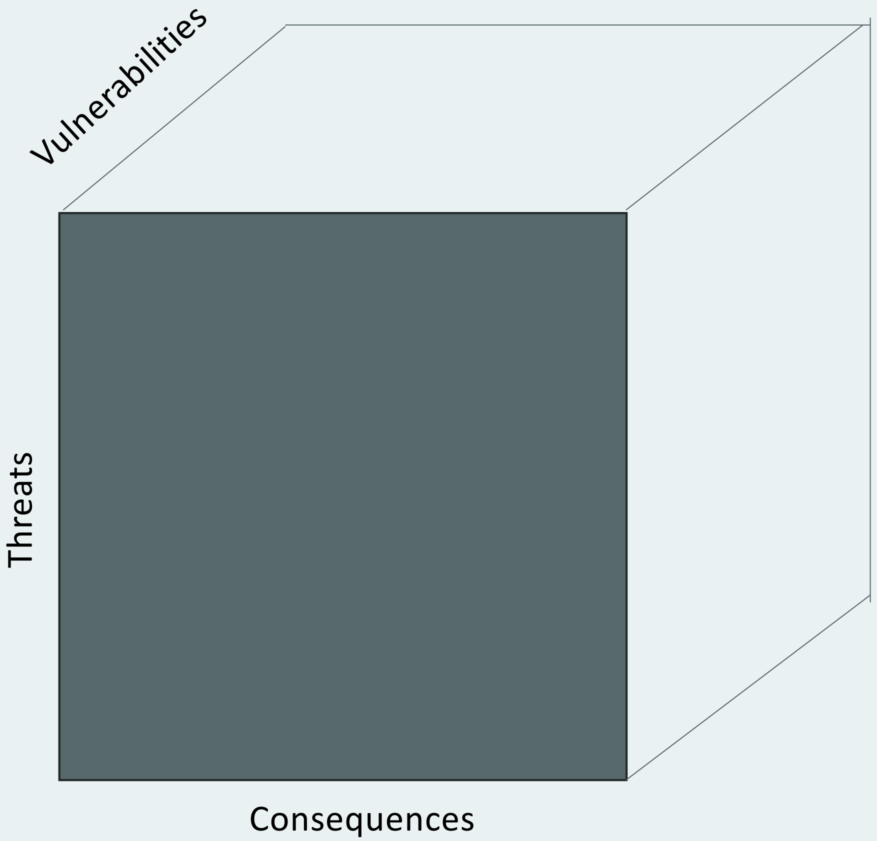
Overview

- Privacy threat modeling
- NIST NCCoE Genomic Data Project
- Privacy threat modeling approach
- What are we doing?
- What could go wrong?
- What do we do about it?
- Conclusion

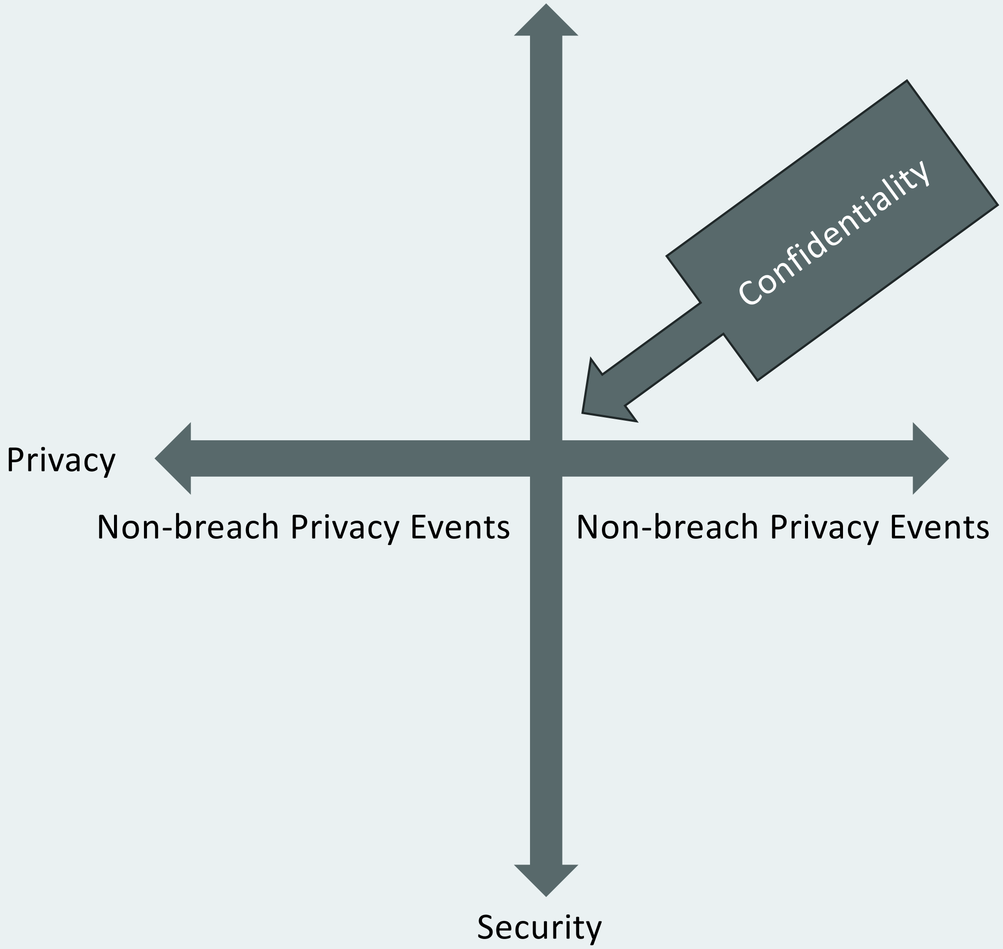
Privacy Threat Modeling

Risk Composition





Privacy vs. Security Risks



Privacy

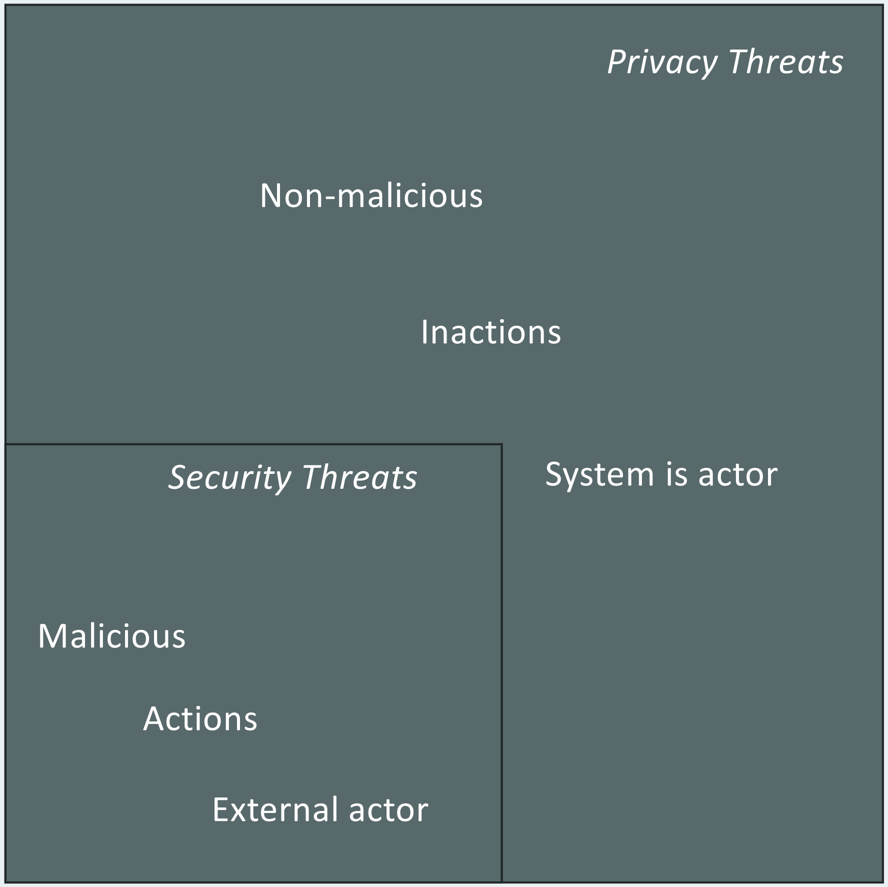
Non-breach Privacy Events

Non-breach Privacy Events

Confidentiality

Security

Privacy vs. Security Threats



Privacy Threats

Non-malicious

Inactions

System is actor

Security Threats

Malicious

Actions

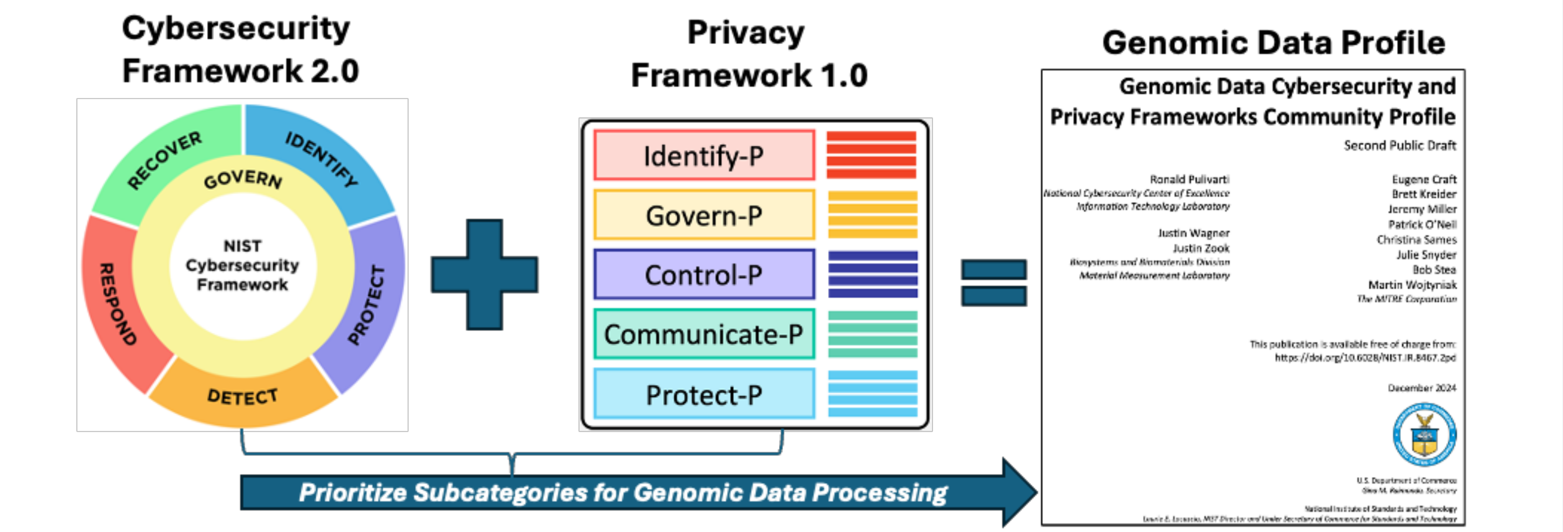
External actor

NIST National Cybersecurity Center of Excellence (NCCoE)Genomic Data Project

Project Summary

- Risk-based cybersecurity and privacy guidelines for the genomic data community
- Cross-stakeholder engagement
  - Government
  - Academia
  - Industry
- Genomic Data and Privacy Frameworks Community Profile
- Privacy Enhancing Technologies (PETs) Testbed
  - Initial focus: privacy-preserving federated learning
- NIST Special Publication (SP) 1800-43, Genomic Data Threat Modeling
  - Volume A: Executive Summary
  - Volume B: Cybersecurity Threat Modeling
  - **Volume C: Privacy Threat Modeling**

Genomic Data Cybersecurity and Privacy Frameworks Community Profile



Genomic Data Cybersecurity and Privacy Frameworks Community Profile

Second Public Draft

Ronald Pulivarti
National Cybersecurity Center of Excellence
Information Technology Laboratory

Justin Wagner
Justin Zook
Biosystems and Biomaterials Division
Material Measurement Laboratory

Eugene Craft
Brett Kreider
Jeremy Miller
Patrick O'Neil
Christina Sames
Julie Snyder
Bob Stea
Martin Wojtyniak
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8467.2pd

December 2024

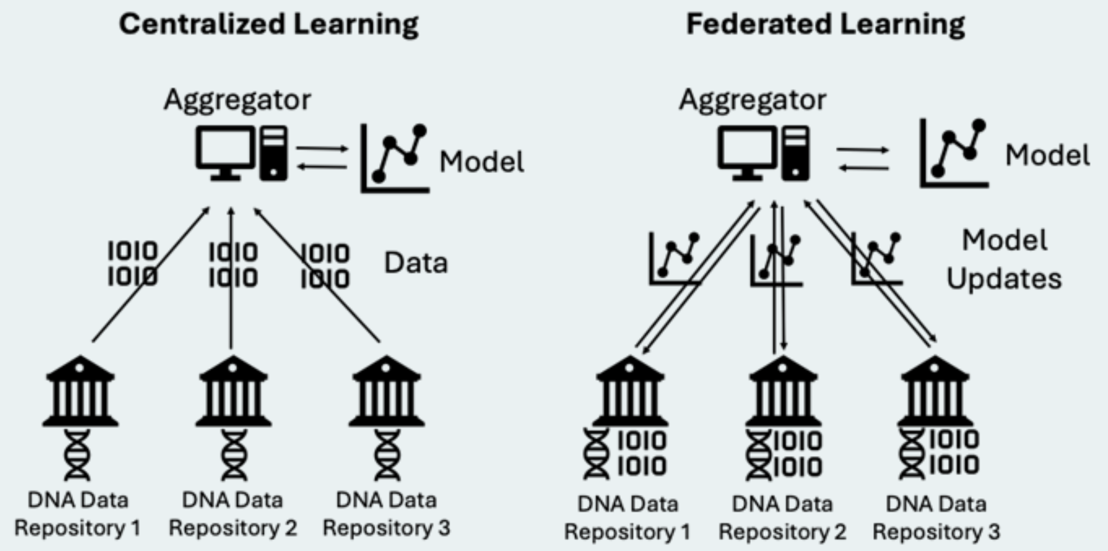
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

The Genomic Data Profile integrates CSF 2.0 and PF 1.0 into a consolidated Community Profile.

NIST NCCoE, "Cybersecurity and Privacy of Genomic Data Factsheet." Available at https://www.nccoe.nist.gov/sites/default/files/2024-12/genomics-fact-sheet.pdf

PETs Testbed

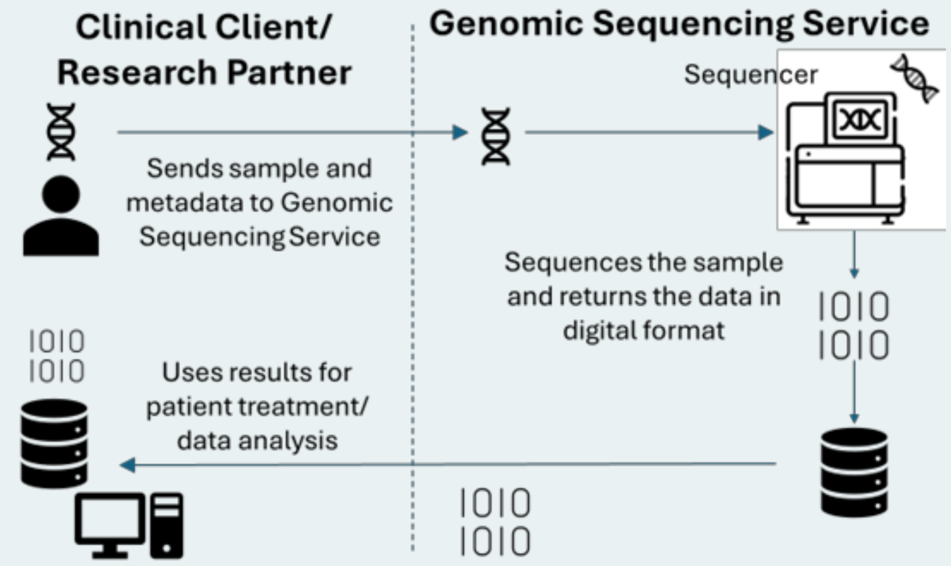


Centralized versus Federated Learning

Federated learning *trains machine learning models across multiple nodes.* ***PPFL*** *is a set of techniques to limit sharing private information across nodes.*

NIST NCCoE, “Cybersecurity and Privacy of Genomic Data Factsheet.” Available at https://www.nccoe.nist.gov/sites/default/files/2024-12/genomics-fact-sheet.pdf

Genomic Data Threat Modeling



Clinical Client/ Research Partner
Genomic Sequencing Service
Sequencer
Sends sample and metadata to Genomic Sequencing Service
Sequences the sample and returns the data in digital format
Uses results for patient treatment/ data analysis
1010
1010

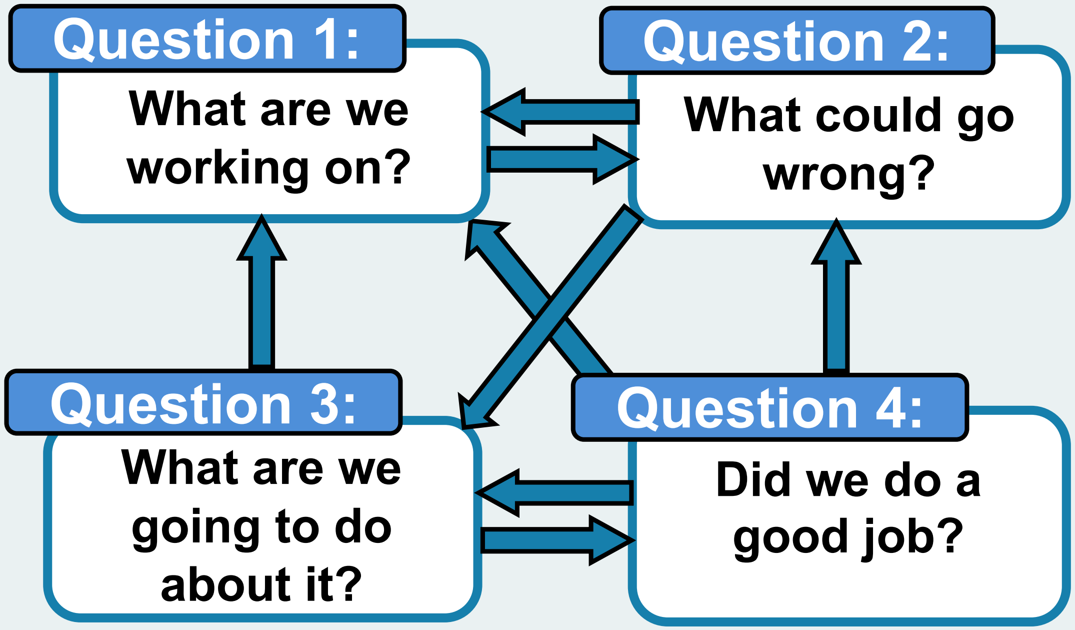
The Genomic Data Sequencing Workflow

*The **Clinical Client/Research Partner** sends a DNA sample to a **Genomic Sequencing Laboratory** that returns the digital results for patient treatment or further analysis.*

NIST NCCoE, "Cybersecurity and Privacy of Genomic Data Factsheet." Available at https://www.nccoe.nist.gov/sites/default/files/2024-12/genomics-fact-sheet.pdf

Privacy Threat Modeling Approach

Four Questions Framework



Question 1: What are we working on?

Question 2: What could go wrong?

Question 3: What are we going to do about it?

Question 4: Did we do a good job?

https://pages.nist.gov/nccoe-genomic-data-threat-modeling/Vol_C/Appendix/appendixC.html

Strategic View

STRIDE

STRIDE Element	Description
Spoofing	Tricking a system into believing a false entity is a true entity
Tampering	Intentional modification of a system or data in an unauthorized manner
Repudiation	Disputing the authenticity of an action taken
Information Disclosure	Exposing information intended to have restricted access levels
Denial of Service (DoS)	Blocking legitimate access to the functionality of a system by malicious process(es)
Elevation of Privilege (EoP)	Gaining access to functions to which an attacker should not normally have access according to the intended security policy

The MITRE Corporation and Medical Device Innovation Consortium (MDIC) (2021), Playbook for Threat Modeling Medical Devices. Available at https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf

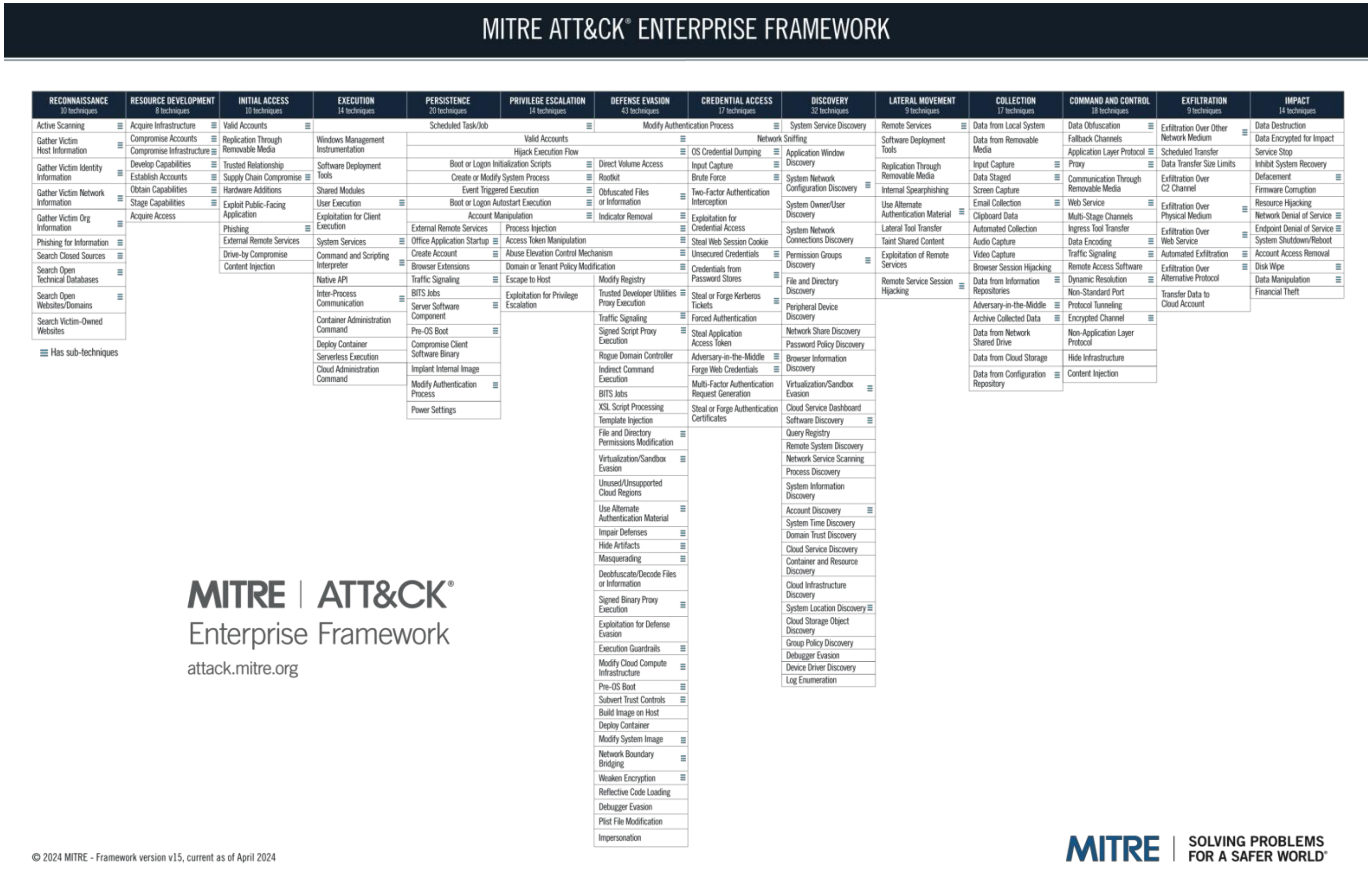
Strategic View

LINDDUN

LINDDUN Element	Description
Linking	Learning more about an individual (or a group) by associating related data items with one another
Identifying	Identity of an individual can be learned through leaks, deduced, or inferred when that is undesirable
Non-repudiation	An individual is unable to deny certain claims pertaining to them as a result of data collected, data shared, or a system action taken by the individual or others Note that this directly conflicts with the repudiation threat type in STRIDE
Detecting	Becoming aware of an individual's involvement, membership, or participation via observation of relevant information
Data Disclosure	Avoidable transfer of an individual's data across a boundary, whether intended or unintended
Unawareness and unintervenability	Insufficiently informing, involving, or empowering the individual with respect to their role and relation to the system
Non-compliance	Lack of adherence to statutory or regulatory requirements or to standards or best practices

https://linddun.org/

Tactical View



MITRE ATT&CK® ENTERPRISE FRAMEWORK

RECONNAISSANCE 10 techniques
- Active Scanning ≡
- Gather Victim Host Information ≡
- Gather Victim Identity Information ≡
- Gather Victim Network Information ≡
- Gather Victim Org Information ≡
- Phishing for Information ≡
- Search Closed Sources ≡
- Search Open Technical Databases ≡
- Search Open Websites/Domains ≡
- Search Victim-Owned Websites

RESOURCE DEVELOPMENT 8 techniques
- Acquire Infrastructure ≡
- Compromise Accounts ≡
- Compromise Infrastructure ≡
- Develop Capabilities ≡
- Establish Accounts ≡
- Obtain Capabilities ≡
- Stage Capabilities ≡
- Acquire Access

INITIAL ACCESS 10 techniques
- Valid Accounts ≡
- Replication Through Removable Media
- Trusted Relationship
- Supply Chain Compromise ≡
- Hardware Additions
- Exploit Public-Facing Application
- Phishing ≡
- External Remote Services
- Drive-by Compromise
- Content Injection

EXECUTION 14 techniques
- Scheduled Task/Job ≡
- Windows Management Instrumentation
- Software Deployment Tools
- Shared Modules
- User Execution ≡
- Exploitation for Client Execution
- System Services ≡
- Command and Scripting Interpreter ≡
- Native API
- Inter-Process Communication ≡
- Container Administration Command
- Deploy Container
- Serverless Execution
- Cloud Administration Command

PERSISTENCE 20 techniques
- Scheduled Task/Job ≡
- Valid Accounts ≡
- Hijack Execution Flow ≡
- Boot or Logon Initialization Scripts ≡
- Create or Modify System Process ≡
- Event Triggered Execution ≡
- Boot or Logon Autostart Execution ≡
- Account Manipulation ≡
- External Remote Services
- Office Application Startup ≡
- Create Account ≡
- Browser Extensions
- Traffic Signaling ≡
- BITS Jobs
- Server Software Component ≡
- Pre-OS Boot ≡
- Compromise Client Software Binary
- Implant Internal Image
- Modify Authentication Process ≡
- Power Settings

PRIVILEGE ESCALATION 14 techniques
- Scheduled Task/Job ≡
- Valid Accounts ≡
- Hijack Execution Flow ≡
- Boot or Logon Initialization Scripts ≡
- Create or Modify System Process ≡
- Event Triggered Execution ≡
- Boot or Logon Autostart Execution ≡
- Account Manipulation ≡
- Process Injection ≡
- Access Token Manipulation ≡
- Abuse Elevation Control Mechanism ≡
- Domain or Tenant Policy Modification ≡
- Escape to Host
- Exploitation for Privilege Escalation

DEFENSE EVASION 43 techniques
- Modify Authentication Process ≡
- Valid Accounts ≡
- Hijack Execution Flow ≡
- Direct Volume Access
- Rootkit
- Obfuscated Files or Information ≡
- Indicator Removal ≡
- Process Injection ≡
- Access Token Manipulation ≡
- Abuse Elevation Control Mechanism ≡
- Domain or Tenant Policy Modification ≡
- Modify Registry
- Trusted Developer Utilities Proxy Execution ≡
- Traffic Signaling ≡
- Signed Script Proxy Execution ≡
- Rogue Domain Controller
- Indirect Command Execution
- BITS Jobs
- XSL Script Processing
- Template Injection
- File and Directory Permissions Modification ≡
- Virtualization/Sandbox Evasion ≡
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material ≡
- Impair Defenses ≡
- Hide Artifacts ≡
- Masquerading ≡
- Deobfuscate/Decode Files or Information
- Signed Binary Proxy Execution ≡
- Exploitation for Defense Evasion
- Execution Guardrails ≡
- Modify Cloud Compute Infrastructure ≡
- Pre-OS Boot ≡
- Subvert Trust Controls ≡
- Build Image on Host
- Deploy Container
- Modify System Image ≡
- Network Boundary Bridging ≡
- Weaken Encryption ≡
- Reflective Code Loading
- Debugger Evasion
- Plist File Modification
- Impersonation

CREDENTIAL ACCESS 17 techniques
- Modify Authentication Process ≡
- Network Sniffing
- OS Credential Dumping ≡
- Input Capture ≡
- Brute Force ≡
- Two-Factor Authentication Interception
- Exploitation for Credential Access
- Steal Web Session Cookie
- Unsecured Credentials ≡
- Credentials from Password Stores ≡
- Steal or Forge Kerberos Tickets ≡
- Forced Authentication
- Steal Application Access Token
- Adversary-in-the-Middle ≡
- Forge Web Credentials ≡
- Multi-Factor Authentication Request Generation
- Steal or Forge Authentication Certificates

DISCOVERY 32 techniques
- System Service Discovery
- Network Sniffing
- Application Window Discovery
- System Network Configuration Discovery ≡
- System Owner/User Discovery
- System Network Connections Discovery
- Permission Groups Discovery ≡
- File and Directory Discovery
- Peripheral Device Discovery
- Network Share Discovery
- Password Policy Discovery
- Browser Information Discovery
- Virtualization/Sandbox Evasion ≡
- Cloud Service Dashboard
- Software Discovery ≡
- Query Registry
- Remote System Discovery
- Network Service Scanning
- Process Discovery
- System Information Discovery
- Account Discovery ≡
- System Time Discovery
- Domain Trust Discovery
- Cloud Service Discovery
- Container and Resource Discovery
- Cloud Infrastructure Discovery
- System Location Discovery ≡
- Cloud Storage Object Discovery
- Group Policy Discovery
- Debugger Evasion
- Device Driver Discovery
- Log Enumeration

LATERAL MOVEMENT 9 techniques
- Remote Services ≡
- Software Deployment Tools
- Replication Through Removable Media
- Internal Spearphishing
- Use Alternate Authentication Material ≡
- Lateral Tool Transfer
- Taint Shared Content
- Exploitation of Remote Services
- Remote Service Session Hijacking ≡

COLLECTION 17 techniques
- Data from Local System
- Data from Removable Media
- Input Capture ≡
- Data Staged ≡
- Screen Capture
- Email Collection ≡
- Clipboard Data
- Automated Collection
- Audio Capture
- Video Capture
- Browser Session Hijacking
- Data from Information Repositories ≡
- Adversary-in-the-Middle ≡
- Archive Collected Data ≡
- Data from Network Shared Drive
- Data from Cloud Storage
- Data from Configuration Repository ≡

COMMAND AND CONTROL 18 techniques
- Data Obfuscation ≡
- Fallback Channels
- Application Layer Protocol ≡
- Proxy ≡
- Communication Through Removable Media
- Web Service ≡
- Multi-Stage Channels
- Ingress Tool Transfer
- Data Encoding ≡
- Traffic Signaling ≡
- Remote Access Software
- Dynamic Resolution ≡
- Non-Standard Port
- Protocol Tunneling
- Encrypted Channel ≡
- Non-Application Layer Protocol
- Hide Infrastructure
- Content Injection

EXFILTRATION 9 techniques
- Exfiltration Over Other Network Medium ≡
- Scheduled Transfer
- Data Transfer Size Limits
- Exfiltration Over C2 Channel
- Exfiltration Over Physical Medium ≡
- Exfiltration Over Web Service ≡
- Automated Exfiltration ≡
- Exfiltration Over Alternative Protocol ≡
- Transfer Data to Cloud Account

IMPACT 14 techniques
- Data Destruction
- Data Encrypted for Impact
- Service Stop
- Inhibit System Recovery
- Defacement ≡
- Firmware Corruption
- Resource Hijacking
- Network Denial of Service ≡
- Endpoint Denial of Service ≡
- System Shutdown/Reboot
- Account Access Removal
- Disk Wipe ≡
- Data Manipulation ≡
- Financial Theft

≡ Has sub-techniques

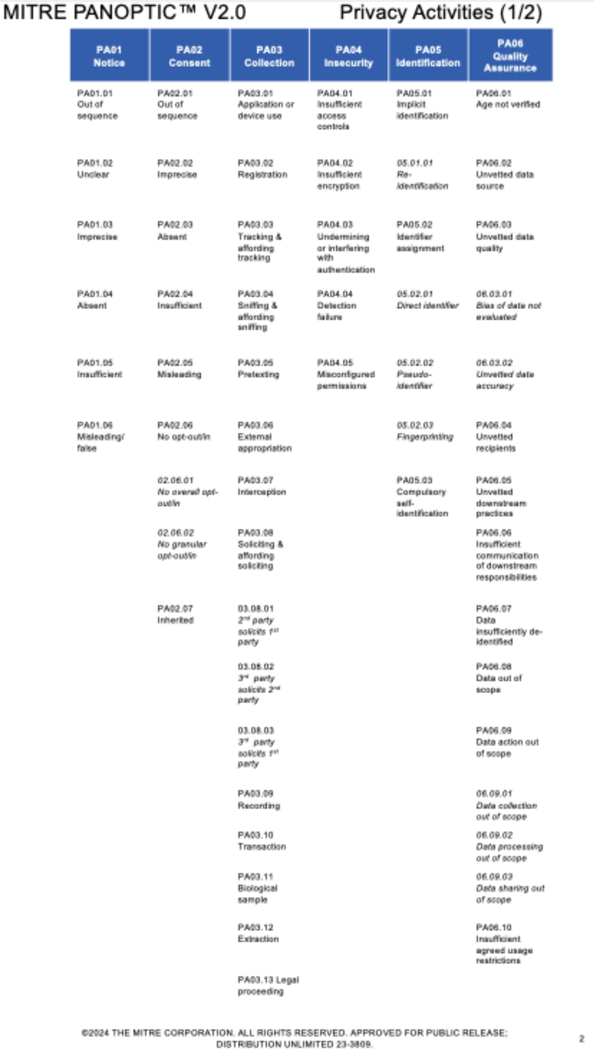
MITRE | ATT&CK®
Enterprise Framework
attack.mitre.org

© 2024 MITRE - Framework version v15, current as of April 2024

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

https://attack.mitre.org/

Tactical View



MITRE PANOPTIC™ V2.0 Privacy Activities (1/2)

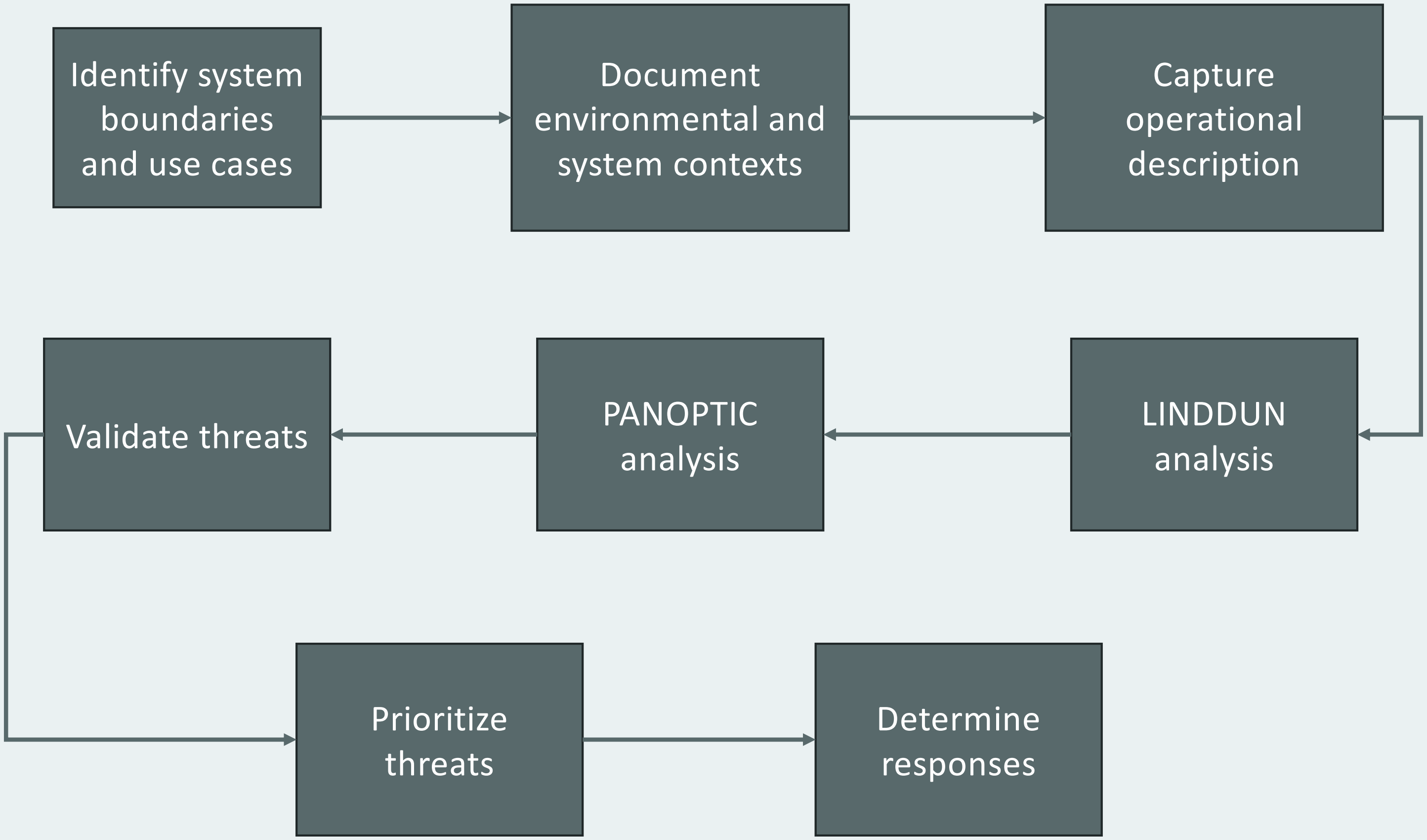
PA01 Notice	PA02 Consent	PA03 Collection	PA04 Insecurity	PA05 Identification	PA06 Quality Assurance
PA01.01 Out of sequence	PA02.01 Out of sequence	PA03.01 Application or device use	PA04.01 Insufficient access controls	PA05.01 Implicit identification	PA06.01 Age not verified
PA01.02 Unclear	PA02.02 Imprecise	PA03.02 Registration	PA04.02 Insufficient encryption	*05.01.01* *Re-identification*	PA06.02 Unvetted data source
PA01.03 Imprecise	PA02.03 Absent	PA03.03 Tracking & affording tracking	PA04.03 Undermining or interfering with authentication	PA05.02 Identifier assignment	PA06.03 Unvetted data quality
PA01.04 Absent	PA02.04 Insufficient	PA03.04 Sniffing & affording sniffing	PA04.04 Detection failure	*05.02.01* *Direct identifier*	*06.03.01* *Bias of data not evaluated*
PA01.05 Insufficient	PA02.05 Misleading	PA03.05 Pretexting	PA04.05 Misconfigured permissions	*05.02.02* *Pseudo-identifier*	*06.03.02* *Unvetted data accuracy*
PA01.06 Misleading/ false	PA02.06 No opt-out/in	PA03.06 External appropriation		*05.02.03* *Fingerprinting*	PA06.04 Unvetted recipients
	02.06.01 *No overall opt-out/in*	PA03.07 Interception		PA05.03 Compulsory self-identification	PA06.05 Unvetted downstream practices
	02.06.02 *No granular opt-out/in*	PA03.08 Soliciting & affording soliciting			PA06.06 Insufficient communication of downstream responsibilities
	PA02.07 Inherited	03.08.01 *2nd party solicits 1st party*			PA06.07 Data insufficiently de-identified
		03.08.02 *3rd party solicits 2nd party*			PA06.08 Data out of scope
		03.08.03 *3rd party solicits 1st party*			PA06.09 Data action out of scope
		PA03.09 Recording			*06.09.01* *Data collection out of scope*
		PA03.10 Transaction			*06.09.02* *Data processing out of scope*
		PA03.11 Biological sample			*06.09.03* *Data sharing out of scope*
		PA03.12 Extraction			PA06.10 Insufficient agreed usage restrictions
		PA03.13 Legal proceeding			

https://ptmworkshop.gitlab.io/#/panoptic

Supporting Players

- NIST Privacy Risk Assessment Methodology (PRAM)
- NIST Privacy Framework v1.0
- NIST Genomic Data Profile
- NIST Special Publication 800-53r5
- NIST Privacy Framework – SP 800-53r5 mapping

Process Flow (Questions 1 – 3)


Identify system boundaries and use cases
Document environmental and system contexts
Capture operational description
LINDDUN analysis
PANOPTIC analysis
Validate threats
Prioritize threats
Determine responses

What are we doing?

Environmental Context

- PRAM Worksheet 1
  - Task 1: Frame organizational objectives
    - Mission needs, functional capabilities, privacy-related goals
  - Task 2: Frame organizational privacy governance
    - Legal environment, privacy-related commitments and policies, risk tolerance
- PRAM Worksheet 2
  - Contextual factors for organization
  - Contextual factors for individuals
- *For each use case: clinical and research*

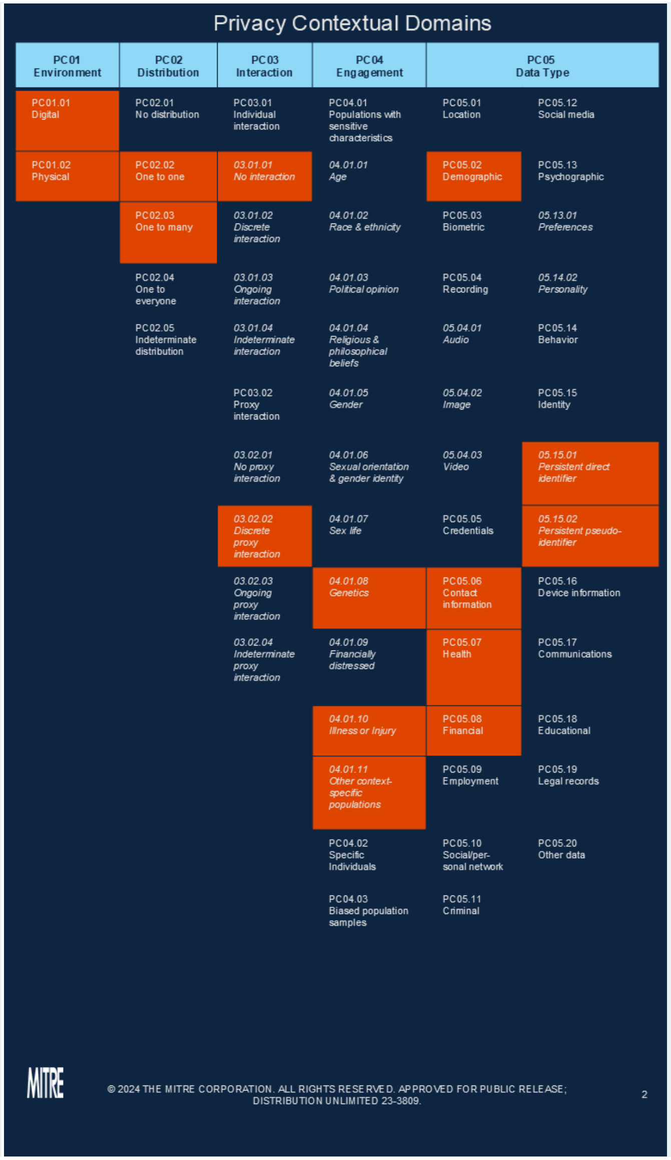
System Context (1/2)

- PRAM Worksheet 2
  - System privacy capabilities for
    - Predictability
    - Manageability
    - Disassociability
  - System contextual factors
- *For each use case: clinical and research*

- Privacy threat: “[A]ny circumstance or event with the potential to compromise the predictability, manageability, and/or disassociability of systems involving data associated with individuals.”*

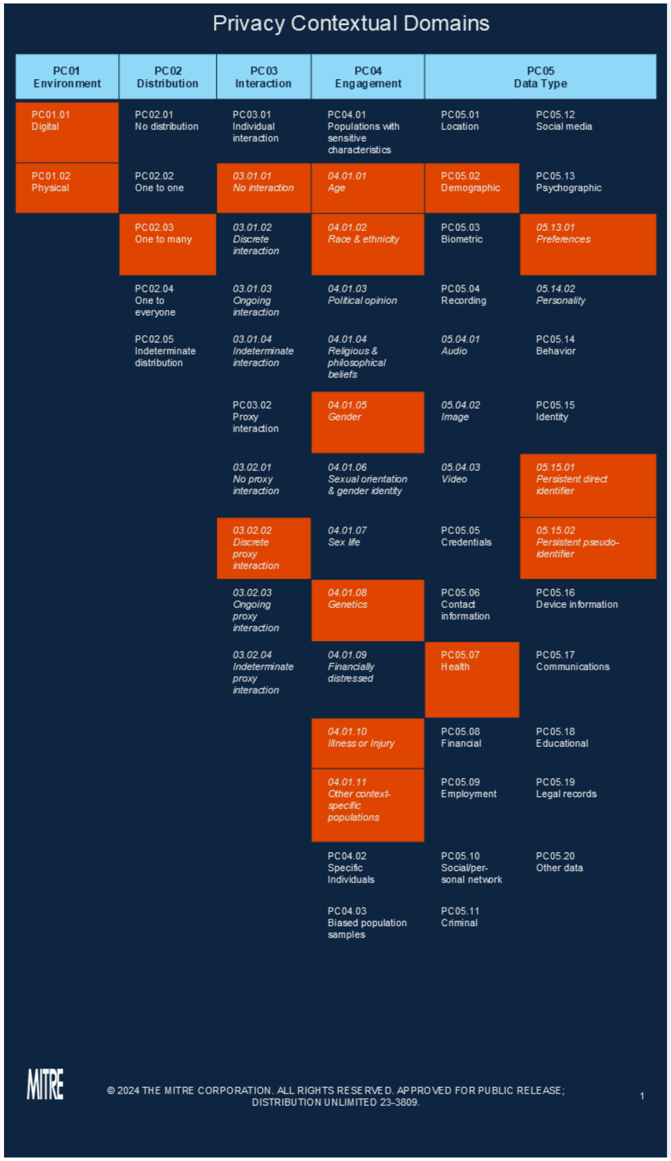
*Pulivarti R, Wagner J, Kreider B, Shapiro S, Snyder J, Wilson K, Wojtyniak M, Ross S, Whitlow P, Brown-Cantrell I, Pape P, Sheldon J (2025) Genomic Data Threat Modeling: Privacy: An implementation for genomic data sequencing and analysis. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 1800-43C ipd. Available at https://www.nccoe.nist.gov/sites/default/files/2025-08/nist-sp-1800-43c-draft.pdf

System Context (2/2)



Privacy Contextual Domains

PC01 Environment	PC02 Distribution	PC03 Interaction	PC04 Engagement	PC05 Data Type	
PC01.01 Digital	PC02.01 No distribution	PC03.01 Individual interaction	PC04.01 Populations with sensitive characteristics	PC05.01 Location	PC05.12 Social media
PC01.02 Physical	**PC02.02 One to one**	***03.01.01 No interaction***	*04.01.01 Age*	**PC05.02 Demographic**	PC05.13 Psychographic
	PC02.03 One to many	*03.01.02 Discrete interaction*	*04.01.02 Race & ethnicity*	PC05.03 Biometric	*05.13.01 Preferences*
	PC02.04 One to everyone	*03.01.03 Ongoing interaction*	*04.01.03 Political opinion*	PC05.04 Recording	*05.14.02 Personality*
	PC02.05 Indeterminate distribution	*03.01.04 Indeterminate interaction*	*04.01.04 Religious & philosophical beliefs*	*05.04.01 Audio*	PC05.14 Behavior
		PC03.02 Proxy interaction	*04.01.05 Gender*	*05.04.02 Image*	PC05.15 Identity
		03.02.01 No proxy interaction	*04.01.06 Sexual orientation & gender identity*	*05.04.03 Video*	***05.15.01 Persistent direct identifier***
		03.02.02 Discrete proxy interaction	*04.01.07 Sex life*	PC05.05 Credentials	***05.15.02 Persistent pseudo-identifier***
		03.02.03 Ongoing proxy interaction	***04.01.08 Genetics***	**PC05.06 Contact information**	PC05.16 Device information
		03.02.04 Indeterminate proxy interaction	*04.01.09 Financially distressed*	**PC05.07 Health**	PC05.17 Communications
			04.01.10 Illness or Injury	**PC05.08 Financial**	PC05.18 Educational
			04.01.11 Other context-specific populations	PC05.09 Employment	PC05.19 Legal records
			PC04.02 Specific Individuals	PC05.10 Social/personal network	PC05.20 Other data
			PC04.03 Biased population samples	PC05.11 Criminal	

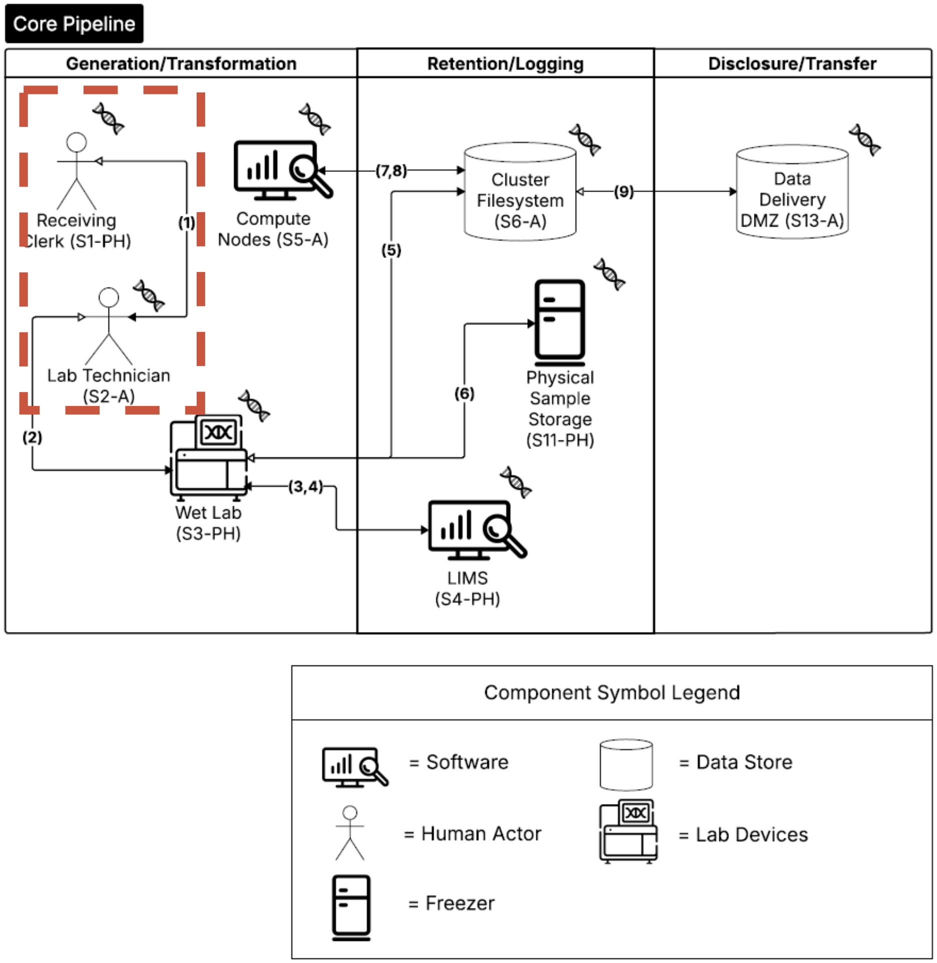


Privacy Contextual Domains

PC01 Environment	PC02 Distribution	PC03 Interaction	PC04 Engagement	PC05 Data Type	
PC01.01 Digital	PC02.01 No distribution	PC03.01 Individual interaction	PC04.01 Populations with sensitive characteristics	PC05.01 Location	PC05.12 Social media
PC01.02 Physical	PC02.02 One to one	***03.01.01 No interaction***	***04.01.01 Age***	**PC05.02 Demographic**	PC05.13 Psychographic
	PC02.03 One to many	*03.01.02 Discrete interaction*	***04.01.02 Race & ethnicity***	PC05.03 Biometric	***05.13.01 Preferences***
	PC02.04 One to everyone	*03.01.03 Ongoing interaction*	*04.01.03 Political opinion*	PC05.04 Recording	*05.14.02 Personality*
	PC02.05 Indeterminate distribution	*03.01.04 Indeterminate interaction*	*04.01.04 Religious & philosophical beliefs*	*05.04.01 Audio*	PC05.14 Behavior
		PC03.02 Proxy interaction	***04.01.05 Gender***	*05.04.02 Image*	PC05.15 Identity
		03.02.01 No proxy interaction	*04.01.06 Sexual orientation & gender identity*	*05.04.03 Video*	***05.15.01 Persistent direct identifier***
		03.02.02 Discrete proxy interaction	*04.01.07 Sex life*	PC05.05 Credentials	***05.15.02 Persistent pseudo-identifier***
		03.02.03 Ongoing proxy interaction	***04.01.08 Genetics***	PC05.06 Contact information	PC05.16 Device information
		03.02.04 Indeterminate proxy interaction	*04.01.09 Financially distressed*	**PC05.07 Health**	PC05.17 Communications
			04.01.10 Illness or Injury	PC05.08 Financial	PC05.18 Educational
			04.01.11 Other context-specific populations	PC05.09 Employment	PC05.19 Legal records
			PC04.02 Specific Individuals	PC05.10 Social/personal network	PC05.20 Other data
			PC04.03 Biased population samples	PC05.11 Criminal	

https://pages.nist.gov/nccoe-genomic-data-threat-modeling/Vol_C/Appendix/appendixE.html

Operational Description*



Data Action Key

1. Receiving Clerk delivers the biological sample to Lab Technician
2. Lab Technician runs the biological sample through the Wet Lab to be transformed into digital data
3. The LIMS is used to track the sample before being de-identified so that the results can then be re-identified after the data has been generated
4. The LIMS returns a de-identified ID to be used for the sample
5. Digital data are transferred to the Cluster Filesystem for use and retention
6. Excess physical samples are moved to Physical Sample Storage for retention according to contextual physical sample retention needs
7. Compute Nodes operate on data to transform it into objective-specific data
8. Objective-specific data is moved from the Compute Nodes and saved on the Cluster Filesystem
9. Objective-specific data is copied to the Data Delivery DMZ, while the data still remains on the Cluster Filesystem according to contextual data retention needs

Management Symbol Legend

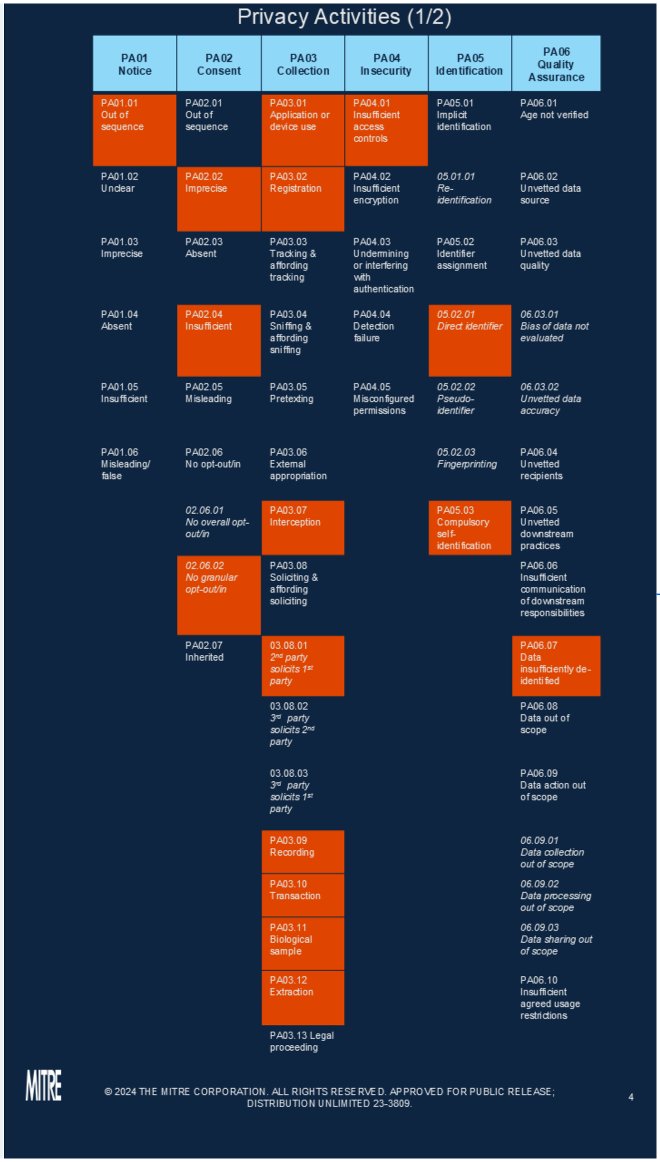
🧬 = Sequencing Lab Managed

What could go wrong?

LINDDUN Analysis*

No.	Source	Dataflow Type	Data Action 1	Data Action 2	Destination	Context (Purpose)	Applicable LINDDUN Threats	
1	Receiving Clerk (S1-PH)	Physical sample	Transfer		Lab Tech (S2-A)	Send physical sample to lab tech for research project	L2.2.1	Sending samples to wet lab known to be researching a specific disease at that time could link samples to that disease

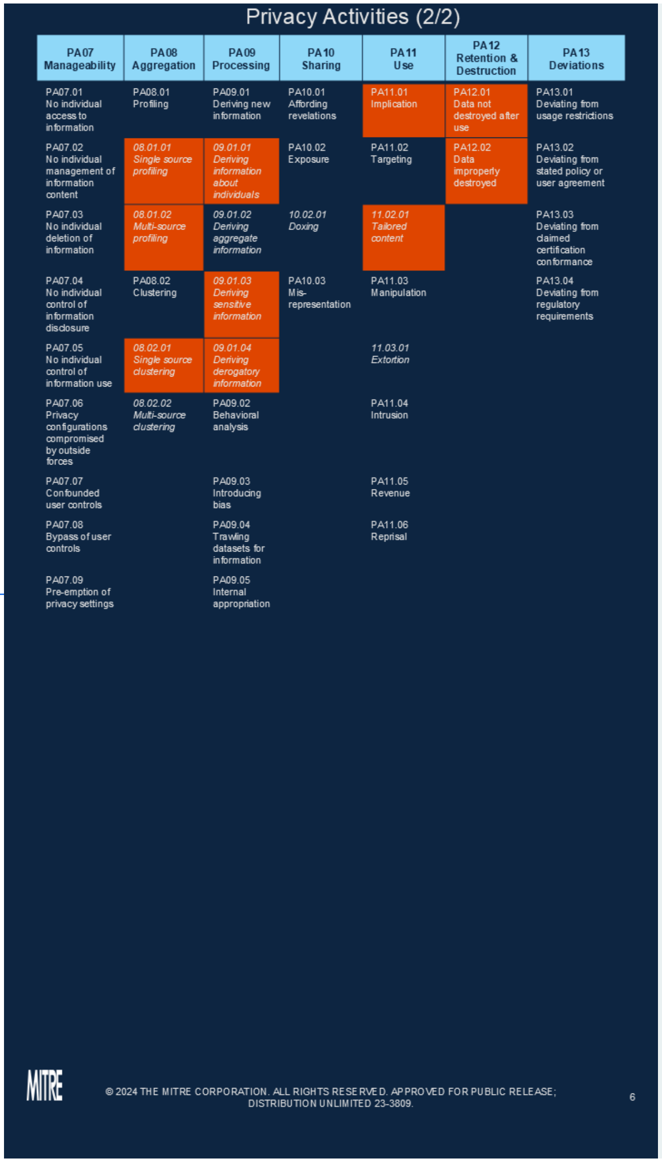
PANOPTIC Analysis



Privacy Activities (1/2)

PA01 Notice	PA02 Consent	PA03 Collection	PA04 Insecurity	PA05 Identification	PA06 Quality Assurance
PA01.01 Out of sequence	PA02.01 Out of sequence	PA03.01 Application or device use	PA04.01 Insufficient access controls	PA05.01 Implicit identification	PA06.01 Age not verified
PA01.02 Unclear	PA02.02 Imprecise	PA03.02 Registration	PA04.02 Insufficient encryption	*05.01.01 Re-identification*	PA06.02 Unvetted data source
PA01.03 Imprecise	PA02.03 Absent	PA03.03 Tracking & affording tracking	PA04.03 Undermining or interfering with authentication	PA05.02 Identifier assignment	PA06.03 Unvetted data quality
PA01.04 Absent	PA02.04 Insufficient	PA03.04 Sniffing & affording sniffing	PA04.04 Detection failure	*05.02.01 Direct identifier*	*06.03.01 Bias of data not evaluated*
PA01.05 Insufficient	PA02.05 Misleading	PA03.05 Pretexting	PA04.05 Misconfigured permissions	*05.02.02 Pseudo-identifier*	*06.03.02 Unvetted data accuracy*
PA01.06 Misleading/ false	PA02.06 No opt-out/in	PA03.06 External appropriation		*05.02.03 Fingerprinting*	PA06.04 Unvetted recipients
	02.06.01 No overall opt-out/in	PA03.07 Interception		PA05.03 Compulsory self-identification	PA06.05 Unvetted downstream practices
	02.06.02 No granular opt-out/in	PA03.08 Soliciting & affording soliciting			PA06.06 Insufficient communication of downstream responsibilities
	PA02.07 Inherited	03.08.01 *2nd party solicits 1st party*			PA06.07 Data insufficiently de-identified
		03.08.02 *3rd party solicits 2nd party*			PA06.08 Data out of scope
		03.08.03 *3rd party solicits 1st party*			PA06.09 Data action out of scope
		PA03.09 Recording			*06.09.01 Data collection out of scope*
		PA03.10 Transaction			*06.09.02 Data processing out of scope*
		PA03.11 Biological sample			*06.09.03 Data sharing out of scope*
		PA03.12 Extraction			PA06.10 Insufficient agreed usage restrictions
		PA03.13 Legal proceeding			

4



Privacy Activities (2/2)

PA07 Manageability	PA08 Aggregation	PA09 Processing	PA10 Sharing	PA11 Use	PA12 Retention & Destruction	PA13 Deviations
PA07.01 No individual access to information	PA08.01 Profiling	PA09.01 Deriving new information	PA10.01 Affording revelations	PA11.01 Implication	PA12.01 Data not destroyed after use	PA13.01 Deviating from usage restrictions
PA07.02 No individual management of information content	*08.01.01 Single source profiling*	*09.01.01 Deriving information about individuals*	PA10.02 Exposure	PA11.02 Targeting	PA12.02 Data improperly destroyed	PA13.02 Deviating from stated policy or user agreement
PA07.03 No individual deletion of information	*08.01.02 Multi-source profiling*	*09.01.02 Deriving aggregate information*	*10.02.01 Doxing*	*11.02.01 Tailored content*		PA13.03 Deviating from claimed certification conformance
PA07.04 No individual control of information disclosure	PA08.02 Clustering	*09.01.03 Deriving sensitive information*	PA10.03 Mis-representation	PA11.03 Manipulation		PA13.04 Deviating from regulatory requirements
PA07.05 No individual control of information use	*08.02.01 Single source clustering*	*09.01.04 Deriving derogatory information*		*11.03.01 Extortion*		
PA07.06 Privacy configurations compromised by outside forces	*08.02.02 Multi-source clustering*	PA09.02 Behavioral analysis		PA11.04 Intrusion		
PA07.07 Confounded user controls		PA09.03 Introducing bias		PA11.05 Revenue		
PA07.08 Bypass of user controls		PA09.04 Trawling datasets for information		PA11.06 Reprisal		
PA07.09 Pre-emption of privacy settings		PA09.05 Internal appropriation				

6

https://pages.nist.gov/nccoe-genomic-data-threat-modeling/Vol_C/Appendix/appendixE.html

Validation*

PA01 Notice	**PA02 Consent**	**PA03 Collection**	**PA04 Insecurity**	**PA05 Identification**	**PA06 Quality Assurance**	**PA07 Manageability**	**PA08 Aggregation**	**PA09 Processing**	**PA10 Sharing**	**PA11 Use**	**PA12 Retention & Destruction**	**PA13 Deviations**

Attack	Scenario	Threat	LINDDUN Analysis	Implicated Privacy Engineering Objectives
PA03.09 PA03.11 PA08.01.01 PA10.01 PA11.01	S1.1	L2.2.1	Sending samples to wet lab known to be researching a specific disease at that time could link samples to that disease	Predictability Disassociability

PA03.09 Recording	PA03.11 Biological sample	PA08.01.01 Single source profiling	PA10.01 Affording revelations	PA11.01 Implication

What are we going to do about it?

Prioritization*

Difficulty Feasibility	Negligible	Minor	Moderate	Significant	Severe
Plausible	1.0	0.8	0.6	0.4	0.2
Indeterminate	0.9	0.7	0.5	0.3	0.1
Implausible	0.8	0.6	0.4	0.2	0.0

LINDDUN Threat Type	Weight
Data Disclosure	1.0
Identifying	0.85
Linking	0.7
Non-compliance	0.5
Unawareness and Unintervenability	0.5
Detecting	0.3
Non-repudiation	0.2

No.	LINDDUN Threat	Feasibility	Difficulty	Ranking Value
55	DD.4.1.2	Plausible	Minor	0.80
5	L.2.1.2	Plausible	Minor	0.56
26	I.2.1.1	Plausible	Moderate	0.51
1	L.2.1.2	Plausible	Moderate	0.42
3	L.2.1.2	Plausible	Moderate	0.42
4	L2.1.2	Plausible	Moderate	0.42
14	L.2.2.1	Plausible	Moderate	0.42
15	L.2.2.1	Plausible	Moderate	0.42
65	U.1.1	Plausible	Minor	0.40
2	L.2.1.2	Plausible	Significant	0.28

Physical samples or raw sequencing data

Options

- Eliminate
- Disrupt
- Transfer responsibility
- Accept

Potential Controls*

PANOPTIC Threat Action	Privacy Framework Sub-Categories	SP 800-53 Controls
PA08.01.01 Aggregation: Profiling: Single source profiling	**Disassociated Processing CT.DP-P2** Data are processed to limit the identification of individuals [1 2 1 2]	**Identification & Authentication IA-4(8)** Pairwise Pseudonymous Identifiers – Generate pairwise pseudonymous identifiers. **System & Information Integrity SI-12(1)** Limit Personally Identifiable Information Elements – Limit personally identifiable information being processed in the information life cycle to the following elements of PII: [Assignment: organization-defined elements of personally identifiable information].
	Protective Technology PR.PT-P2 The principle of least functionality is incorporated by configuring systems to provide only essential capabilities [3 2 2 2]	**Configuration Management CM-7** Least Functionality – Configure the system to provide only [Assignment: organization-defined mission essential capabilities].
	Disassociated Processing CT.DP-P3 Data are processed to limit the formulation of inferences about individuals' behavior or activities [2 3 2 2]	**Audit & Accountability AU-16(3)** Disassociability – Implement [Assignment: organization-defined measures] to disassociate individuals from audit information transmitted across organizational boundaries.

Conclusion

Takeaways

- Privacy threat modeling identifies privacy threats to data subjects, including those posed by the system itself
- Potential risk is addressed at the earliest possible point: at the origin of the risk chain
- Privacy threat modeling complements cybersecurity threat modeling but is distinct

Ordinary mortals can do this, in a reasonable amount of time with a reasonable amount of effort

It’s not a zero-sum game

Resources

- NIST Special Publication 1800-43C (ipd): https://www.nccoe.nist.gov/sites/default/files/2025-08/nist-sp-1800-43c-draft.pdf
  - Appendices: https://pages.nist.gov/nccoe-genomic-data-threat-modeling/
- LINDDUN: https://linddun.org/
- MITRE PANOPTIC™: https://ptmworkshop.gitlab.io/#/panoptic
- NIST Privacy Risk Assessment Methodology (PRAM): https://www.nist.gov/document/nist-pram-feb2019zip
- NIST Privacy Framework v1.0: https://doi.org/10.6028/NIST.CSWP.01162020
- NIST Genomic Data Community Profile (2pd): https://doi.org/10.6028/NIST.IR.8467.2pd
- NIST Special Publication 800-53r5: https://doi.org/10.6028/NIST.SP.800-53r5
- NIST Privacy Framework – SP 800-53r5 mapping: https://csrc.nist.gov/files/pubs/sp/800/53/r5/upd1/final/docs/csf-pf-to-sp800-53r5-mappings.xlsx

Thank you

Stuart Shapiro

+1-603-365-6296

sshapiro@nemojr.com

www.nemojr.com