|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Function | Category | FW | Subcategory | 1.  Data | 2.  Relatives | 3. Risks | 4.  Consent | 5.  Donors | Mission Objective Specific Considerations |
| Govern | Organizational Context | **CSF** | **GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management | 2 | 2 | **1** | 2 | 2 | 2,4,5 - Organizational mission helps to define requirements around consent, donor privacy, and potential impact on relatives. 6,8,12 - Mission informs cybersecurity risk management decisions related to the value of the data used, results from research activities, and the need for or use of new technologies, supporting an organization’s ability to manage impact from adverse events (e.g., unauthorized access) that may affect the mission. 9 - Legal and regulatory compliance enable the organization to achieve its mission. 10,11 - Priorities for protecting IP or ensuring sample diversity in support of the mission are understood. |
| Identify | Business Environment | **PF** | **ID.BE-P2:** Priorities for organizational mission, objectives, and activities are established and communicated. | 3 | 3 | 2 | 3 | 3 | 9 - Prioritize legal compliance to ensure business viability. 10 - Organizations with IP prioritize protecting inventions and investments.11 - Diversity needs vary based on the context of processing and may require coordination with multiple organizations. Clearly communicate priorities related to diversity to influence operations.12 - Priorities determine how forward-leaning the organization is when embracing privacy-enhancing and secure technologies; ID.BE-P1 and -P3 more directly influence technology decisions. |
| Govern | Organizational Context | **CSF** | **GV.OC-02:** Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered | **1** | **1** | **1** | 2 | **1** | 1 - Data quality and provenance require managing any risk introduced by suppliers or partners.2,4,5,8 - Each stakeholder in a genomic data processing relationship understands the relationship between cybersecurity and privacy risk management and expectations for how cybersecurity activities support privacy needs. For example, they understand their responsibilities to protect genomic data according to consent agreements and consider when additional access controls may be necessary to protect more sensitive data. Stakeholders are also aware of where additional measures are necessary to address the full scope of privacy risk by integrating Privacy Framework Subcategories.11 - Partners sharing data consider cybersecurity requirements to ensure that all stakeholders protect and maintain sample diversity. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P2:** Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process. | **1** | 2 | **1** | 3 | **1** | 2,5 - Identify where privacy risks to relatives and donors might arise in the genomic data processing ecosystem, including re-identification. 7 - Implement external risk management activities that foster trust and are supported by all stakeholders sharing data.11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations; manage data diversity across the ecosystem.12 - Technologies support effective, controlled sharing of genomic data. |
| Govern | Organizational Context | **CSF** | **GV.OC-03:** Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed | **1** | **1** | **1** | **1** | **1** | 1,3,8 - Compliance with laws and regulations provides foundational measures that help ensure that risks to data are appropriately managed throughout the life cycle and with partners, using contracts to enforce requirements. Managing risks may require additional measures beyond the minimum requirements expressed in laws, regulations, and contracts.2,4,5 - Failure to comply with cybersecurity or privacy laws and regulations could deter donors from participating.7 - Reputation and trust will be damaged if laws and regulations are not followed.9 - Legal and regulatory requirements are prioritized and enforced through organizational policy, processes, procedures, and contracts.11 - Organizations remain cognizant of evolving legislation related to sample diversity. In the absence of requirements, organizations and affected communities work together to determine needs for specific genomic data processing purposes.12 - Any impact on legal and regulatory compliance will be assessed as part of the acquisition or use of new technologies. |
| Govern | Governance Policies, Processes, and Procedures | **PF** | **GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals’ prerogatives with respect to data processing) are established and communicated. | **1** | **1** | **1** | **1** | **1** | 2,4,5 - Relatives’ privacy can be neglected. High-level policies that influence downstream practices can dictate and enforce privacy protection requirements for donors and relatives, including consent. 3 - Organizational policies can collectively act to protect general bioeconomy interests from adverse outcomes that are identified through risk assessment. 7 - Governance will need to address issues that may not be fully defined in laws and regulations. 6,10,12 - Policies set the expectation for data access management, IP protections, and when and how technologies are used inside the organization. |
| Govern | Governance Policies, Processes, and Procedures | **PF** | **GV.PO-P5:** Legal, regulatory, and contractual requirements regarding privacy are understood and managed. | 2 | 2 | 2 | **1** | **1** | 2 - In some situations where the absence of specific legal requirements for the processing of genomic data may lead to data aggregation and inference (e.g., relatedness), organization-specific policies may be required to address potential privacy harms across an ecosystem. 4 - Consent needs to travel with data, and where specific laws do not address this requirement, policies could be used and incorporated into contracts. 5,11,12 - Even within a certain geography, other specific requirements may be necessary based on use case (e.g., clinical care, disease testing), ethnicity (e.g., Native Nations), or other regulations (HIPAA, GINA). |
| Govern | Organizational Context | **CSF** | **GV.OC-04:** Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated | 2 | 3 | 2 | 3 | 2 | 1,3 - The data life cycle is dependent on data quality to support essential services. The impact of these dependencies will be incorporated into risk management.8 - Genomic researchers depend on sharing between partners and will identify dependencies that may introduce risks.11 - Partners who share data consider stakeholder dependencies that include protecting and maintaining sample diversity throughout the life cycle. 12 - Whenever using new technologies or platforms, organizations will assess any dependencies that may impact the availability or delivery of services. |
| Govern | Organizational Context | **CSF** | **GV.OC-05:** Outcomes, capabilities, and services that the organization depends on are understood and communicated | 2 | 2 | **1** | 3 | 2 | 1,3 - The data life cycle depends on data quality to support essential services. The impact of those dependencies will be incorporated into risk management. 2,4,5 - Privacy outcomes that rely on cybersecurity capabilities are included in dependencies. 7 - Issues with delivering services may result in other organizations losing trust in your organization. 8 - Researchers may not be able to deliver results without the services or sources they depend on.  9 - Organizations assess their role in the delivery of critical services and how legal compliance may be impacted through a disruption of services. 12 - Organizations determine dependencies on new technologies and services that may impact availability or the ability to deliver their own services. |
| Identify | Business Environment | **PF** | **ID.BE-P1:** The organization’s role(s) in the data processing ecosystem are identified and communicated. | 2 | 2 | 2 | 2 | 2 | 2,4,5 - Organizational role can inform management of donor and relative privacy and consent requirements while sharing data. 7 - Context for use, social norms, perceptions, and political issues factor into trust and managing reputation.  8 - Understanding role in the research community supports the sharing of data within the research community, ensuring consent travels with data, monitoring potential risks, and monitoring changes for how data can be used for research across multiple participants. 12 - Technologies prioritize safe and controlled use of genomic data, factoring in the risk profile of data usage and its role in the ecosystem. |
| Govern | Risk Management Strategy | **CSF** | **GV.RM-01:** Risk management objectives are established and agreed to by organizational stakeholders | 2 | 2 | **1** | 2 | 2 | 1,3,10 - Risk management processes are integrated into the data processing life cycle and systems development life cycle. 2,4,5 - Risk management objectives incorporate cybersecurity and privacy objectives and an understanding of how the objectives may impact each other. 7,9 - Processes for managing reputational risk and legal and regulatory requirements are included. 12 - Users of technologies and platforms integrate risk management across all technologies used. |
| Govern | Risk Management Strategy | **PF** | **GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders. | **1** | 2 | **1** | 3 | 2 | 1,12 - Rapid advances in genomic-related technologies and data processing techniques will necessitate ongoing risk assessments to maintain effective application of controls and ensure data quality.  3 - Once a risk assessment is conducted, an organization will need a long-term strategy to guide the implementation of protocols and policies that are aligned with its goals and the protections needed.  8 - Research inherently broadens the reach of data, so risk assessment needs to be thought of as ecosystem-wide rather than limited to one organization.  11 - Risk assessments can help identify issues with sample diversity. |
| Govern | Risk Management Strategy | **CSF** | **GV.RM-02:** Risk appetite and risk tolerance statements are established, communicated, and maintained | **1** | 2 | **1** | 2 | 2 | 1,6,7,10 - Risk tolerance helps define requirements and priorities for provenance, data quality, who can access the data, and what might cause reputational harm. 2,4,5 - Privacy requirements help define risk tolerances. 3 - Risk tolerance informs risk decisions and responses when a risk is realized. 9 - Laws and regulations help define organizational risk tolerance or thresholds. |
| Govern | Risk Management Strategy | **PF** | **GV.RM-P2:** Organizational risk tolerance is determined and clearly expressed. | 2 | 2 | **1** | 3 | 2 | 2 - Risks to relatives, especially around privacy, may be difficult to quantify and instead be based on qualitative considerations such as ethics and social harms, so establishing tolerances into an overall risk management strategy could potentially be set by looking to industry best practices.  10 - The value of IP to an organization is already assumed to be high (and may be more of a cybersecurity issue), so it may not receive as much analysis compared to other privacy risk factors. |
| Govern | Risk Management Strategy | **PF** | **GV.RM-P3:** The organization’s determination of risk tolerance is informed by its role(s) in the data processing ecosystem. | 2 | 2 | **1** | 3 | 2 | 1,8,12 - Organizations may be able to establish privacy protections based on partnership expectations, while they work on defining their own risk tolerance levels. Changes in organizational ownership, partner engagement, technologies implemented, or data processing requirements will affect risk tolerances over time.  10 - Since an organization directly owns and protects its own IP, it will have already established the value and tolerances well in advance of ecosystem considerations. |
| Govern | Risk Management Strategy | **CSF** | **GV.RM-03:** Cybersecurity risk management activities and outcomes are included in enterprise risk management processes | **1** | **1** | **1** | 2 | **1** | 1,3 - Cybersecurity risk management is built into the data life cycle to ensure the organization can complete its mission.  2,4,5 - Cybersecurity risk management addresses certain aspects of privacy risk management. 7 - Cybersecurity risk management processes can help protect trust and reputation.  10 - Cybersecurity risk management processes help identify and prioritize appropriate IP protections required to perform business operations.  12 - New technologies integrate appropriate cybersecurity and privacy risk management capabilities. |
| Govern | Governance Policies, Processes, and Procedures | **PF** | **GV.PO-P6:** Governance and risk management policies, processes, and procedures address privacy risks. | 2 | **1** | **1** | 2 | **1** | 1,5 - Aspects of the data life cycle, such as data-in-use, also introduce risks. Other potential protections (such as homomorphic encryption) are addressed in other Subcategories.  2 - The governance body itself may need to understand the privacy risks to relatives from inferred data techniques, as this is largely a technical issue.  8 - Laws and regulations pertaining to the research ecosystem will also address privacy protections, such as HIPAA and GINA.  11 - Policies and procedures can help achieve an appropriate data diversity that may vary over time and across geographies. |
| Govern | Risk Management Strategy | **CSF** | **GV.RM-04:** Strategic direction that describes appropriate risk response options is established and communicated | 2 | 2 | 2 | 2 | 2 | 1,2,4,5,7,9,10 - These risk responses support the continuity of business operations by addressing protections and requirements for data quality, privacy, consent, reputation, IP, sample diversity, integration with new technologies, and legal risks. |
| Govern | Risk Management Strategy | **PF** | **GV.RM-P2:** Organizational risk tolerance is determined and clearly expressed. | 2 | 2 | **1** | 3 | 2 | 2 - Risks to relatives, especially around privacy, may be difficult to quantify and instead be based on qualitative considerations such as ethics and social harms, so establishing tolerances into an overall risk management strategy could potentially be set by looking to industry best-practices.  10 - The value of IP to an organization is already assumed to be high (and may be more of a cybersecurity issue), so it may not receive as much analysis compared to other privacy risk factors. |
| Govern | Risk Management Strategy | **CSF** | **GV.RM-05:** Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties | **1** | 2 | **1** | 2 | 2 | 2,5 - All organizations in the genomic data supply chain manage privacy risks, including risks from aggregated and anonymized data that may be de-identified. 6 - Data access requirements apply to each organization in the supply chain. 7 - Reputation and trust are managed across all organizations processing the data. 12 - Organizations establish relationships with new technology providers to facilitate managing risks introduced by the technology solution. |
| Communicate | Communication Policies, Processes, and Procedures | **PF** | **CM.PO-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place. | 2 | 2 | 2 | **1** | **1** | 2,4,5,11 - Organizations can maintain the trust of donors and members of communities represented in research studies through proactive communication and notification of any issues that impact consent, privacy, or represented (or unrepresented) populations. Relatives will generally not be able to be notified. 8,10,12 - Researchers, owners of IP, and technology providers will benefit from communication across partners to manage privacy risks and help those using the data regain trust in the data quality, provenance, and research results. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders. | **1** | 2 | 2 | 2 | **1** | 2,4,5 - Identify where privacy risks to relatives or donors might arise in the genomic data processing ecosystem. Consent data will be treated as a high value and requires asset inventory and processing to know what data are subject to informed consent requirements and who can access that data. 11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations. This may be prioritized due to the increased reach of data in research. The data processing environment will manage the appropriate degree of diversity.  12 - Data processing helps manage the effective, controlled sharing of genomic data across various technologies and even helps drive the requirements for technologies. |
| Govern | Risk Management Strategy | **CSF** | **GV.RM-06:** A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated | 2 | 2 | **1** | 2 | 2 | 1,3 - Standardization helps ensure consistent data quality and provenance protections across the data processing life cycle and systems development life cycle. 2,4,5 - Standardization facilitates consistency in managing risk to privacy, reputation, and IP. 12 - Standardization ensures consistent risk management when integrating new technologies. |
| Govern | Risk Management Strategy | **PF** | **GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders. | **1** | 2 | **1** | 3 | 2 | 1,12 - Rapid advances in genomic-related technologies and data processing techniques will necessitate ongoing risk assessments to maintain effective application of controls and ensure data quality.  3 - Once a risk assessment is conducted, an organization will need a long-term strategy to guide the implementation of protocols and policies that are aligned to its goals and to the protections needed.  8 - Research inherently broadens the reach of data, so risk assessment needs to be thought of as ecosystem-wide rather than limited to one organization.  11 - Risk assessments can help identify issues with sample diversity. |
| Govern | Risk Management Strategy | **CSF** | **GV.RM-07:** Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions | 3 | 3 | 2 | 3 | 2 | 7 - Organizations with effective cybersecurity practices can use that capability to demonstrate their ability to be trusted by donors and other organizations and improve their overall market share and impact. 8 - Effective cybersecurity creates a strategic opportunity to demonstrate the trustworthiness of research results and as a research partner. 10 - Effective cybersecurity may be used to improve the marketing and trustworthiness of IP. 12 - New technologies that demonstrate effective cybersecurity practices will have strategic opportunities for marketing their product. |
| Govern | Roles, Responsibilities, and Authorities | **CSF** | **GV.RR-01:** Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving | 2 | 2 | 2 | 2 | 2 | 7 - Reputation management starts at the highest level of the organization and is promoted by instilling a culture that values trust through trustworthy behaviors. 9 - Individuals in organizational leadership roles can be held legally responsible and accountable for organizational risk management strategies, decisions, and guidance that shape cybersecurity culture and compliance. |
| Govern | Roles, Responsibilities, and Authorities | **CSF** | **GV.RR-02:** Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced | 2 | 2 | **1** | 2 | 2 | 1 - Organizations manage data provenance and integrity by clearly articulating personnel responsibilities across the data life cycle, establishing accountability.  2,4,5 - Cybersecurity and privacy functions will be coordinated and supported by clear roles, responsibilities, and authorities, including all partners in the data life cycle. 3 - Clear roles and responsibilities empower personnel to effectively manage cybersecurity risks by setting clear expectations. As an organization's risk posture changes over time, these roles and responsibilities also evolve to address emerging threats, such as insider risks, and to ensure the protection of any new types of information the organization may begin processing 9 - Laws and regulations may stipulate specific cybersecurity and privacy roles and responsibilities (for example, CISO, ISSO, Privacy Officer). |
| Govern | Governance Policies, Processes, and Procedures | **PF** | **GV.PO-P3:** Roles and responsibilities for the workforce are established with respect to privacy. | 3 | 2 | 2 | 2 | 2 | 2,5,6,10 - The workforce will understand the value of the genomic data, including specific privacy considerations and any relevant IP. Role-based specifics of how to manage the data life cycle will be primarily addressed in the Control and Protect functions.  9 - The workforce will clearly understand their role in pertinent legal compliance issues.  12 - New technologies will include appropriate roles to reinforce privacy requirements. |
| Govern | Governance Policies, Processes, and Procedures | **PF** | **GV.PO-P4:** Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners). | 3 | 2 | 2 | 2 | 2 | 1,4,8,12 - Coordination acts to preserve original source (provenance) and privacy rights over the life cycle and across partners. Clear expectations and roles can help address deficiencies in environments where security and privacy are not typically priorities.  2,5 - Coordination across partners will help manage privacy protections specific to donors and relatives. 9 - Legal requirements merit additional prioritization as these issues have a risk profile (reputation, compliance) and can also be difficult to define as they may cover non-technical issues. |
| Govern | Roles, Responsibilities, and Authorities | **CSF** | **GV.RR-03:** Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies | 2 | 2 | **1** | 2 | 2 | 1,3,6,8,10 - Organizations determine how many resources are needed to implement, monitor, and maintain cybersecurity capabilities to meet strategic goals and comply with policies.  2,4,5 - Organizations manage cybersecurity and privacy resources together to ensure that adequate resources are allocated to address both cybersecurity and privacy risk management priorities and needs. |
| Govern | Roles, Responsibilities, and Authorities | **CSF** | **GV.RR-04:** Cybersecurity is included in human resources practices | 3 | 3 | **1** | 3 | 3 | 3,6,10 - These MOs require higher prioritization of personnel screening and management due to insider threat risks, including unauthorized access or IP loss. 8,9,11,12 - Organizations operating shared data environments or managing data stores implement HR policies to address personnel cybersecurity risks. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P9:** Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening). | 2 | 3 | 2 | 2 | 3 | 1,6,12 - Procedures help enforce consistent security practices to manage provenance, ensure data quality, and restrict access. Access controls need to be updated for staff turnover. 4 - Procedures support access management, aligned with consent requirements. 7,9 - HR practices help create a culture of trust in organizations and establish their reputation. Before participating in genomic data activities, potential donors want to know they can trust organizations with their genomic data and the workforce within those organizations charged with safeguarding the data. |
| Govern | Policy | **CSF** | **GV.PO-01:** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced | **1** | **1** | **1** | **1** | **1** | 1 - Policies incorporate data quality and provenance requirements. 2,4,5 - Policies address privacy and consent requirements, including protecting relatives' privacy. 3,6,10 - Policies define required risk management activities, access controls, and IP protections. 11 - Policies help enable and preserve sample diversity.  12 - Policies enforce cybersecurity requirements for technology solutions. |
| Govern | Governance Policies, Processes, and Procedures | **PF** | **GV.PO-P1:** Organizational privacy values and policies (e.g., conditions on data processing such as data uses or retention periods, individuals’ prerogatives with respect to data processing) are established and communicated. | **1** | **1** | **1** | **1** | **1** | 2,4,5 - Relatives’ privacy can be neglected. High-level policies that influence downstream practices can dictate and enforce privacy protection requirements for donors and relatives, including consent.  3 - Organizational policies can collectively act to protect general bioeconomy interests from adverse outcomes that are identified through risk assessment.  7 - Governance will need to address issues that may not be fully defined in laws and regulations.  6,10,12 - Policies set the expectation for data access management, IP protections, and when and how technologies are used inside the organization. |
| Govern | Governance Policies, Processes, and Procedures | **PF** | **GV.PO-P6:** Governance and risk management policies, processes, and procedures address privacy risks. | 2 | **1** | **1** | 2 | **1** | 1 - Policies, processes, and procedures address aspects of the data life cycle such as data-in-use.  2,5 - The governance body itself may need to understand the privacy risks to donors and relatives from inferred data techniques, as this is largely a technical issue.  8 - Laws and regulations pertaining to the research ecosystem will also address privacy protections, such as HIPAA and GINA.  11 - Policies and procedures can help achieve an appropriate data diversity that may vary over time and across geographies. |
| Govern | Policy | **CSF** | **GV.PO-02:** Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission | **1** | 2 | **1** | **1** | 2 | 1,3,6,8,10 - Policy updates help to address newly identified cybersecurity risks to data quality, provenance, access control, research environments, and IP. 2,4,5 - Policy updates help address changes to privacy or consent requirements, threats, and uses, as well as advancements in privacy protections. 12 - Policy updates help manage cybersecurity risks introduced by the use of new technologies. |
| Govern | Monitoring and Review | **PF** | **GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization’s business environment (e.g., introduction of new technologies), governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change. | 2 | **1** | **1** | 2 | **1** | 2,3,4,5 - Conduct privacy risk assessments to assess the impact that changes in technology and regulations may have. Privacy, consent, and relatedness issues may impact dignity loss, discrimination, loss of trust, or loss of autonomy because of unanticipated revelation of health conditions of donors or their kin/progeny. 6 - Automated continuous monitoring of data access is expected to maintain situational awareness and compliance with data breach detection and reporting requirements. 11 - Privacy risks to data sets and sample diversity could impact decisions to share those data sets with certain partners. |
| Govern | Monitoring and Review | **PF** | **GV.MT-P6:** Policies, processes, and procedures incorporate lessons learned from problematic data actions. | 2 | 2 | 2 | 3 | 2 | 12 - An example of incorporating lessons learned from new technologies is the implementation of safeguards against potential problematic data actions from new de-anonymization techniques that could be used to access or aggregate data of a discriminated population. |
| Govern | Oversight | **CSF** | **GV.OV-01:** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction | 2 | 3 | 2 | 3 | 3 | 7,9,10 - Ensure that the strategy reflects priorities to manage trust, reputation, legal compliance, and IP protections. |
| Govern | Oversight | **CSF** | **GV.OV-02:** The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks | 2 | 2 | **1** | 3 | 2 | 1 - Audit findings confirm compliance requirements for data-sharing arrangements among third parties so that protections are met throughout the life cycle. 3 - The cybersecurity risk management strategy dictates the requirements for cybersecurity and risk assessment and will be adjusted as risk assessment findings identify risks. |
| Govern | Risk Management Strategy | **PF** | **GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders. | **1** | 2 | **1** | 3 | 2 | 1,12 - Rapid advances in genomic-related technologies and data processing techniques will necessitate ongoing risk assessments to maintain effective application of controls and ensure data quality.  3 - Once a risk assessment is conducted, an organization will need a long-term strategy to guide the implementation of protocols and policies that are aligned to its goals and to the protections needed.  8 - Research inherently broadens the reach of data, so risk assessment needs to be thought of as ecosystem-wide rather than limited to one organization.  11 - Risk assessments can help identify issues with sample diversity. |
| Govern | Oversight | **CSF** | **GV.OV-03:** Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed | 3 | 3 | **1** | 3 | 2 | 3 - The risk assessment process is adjusted to identify and address deficiencies in the overall cybersecurity risk management program. 10 - Outcomes from performance evaluations ensure appropriate adjustments are made to protect IP. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-01:** A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders | **1** | 2 | **1** | 2 | 2 | 2,4,5 - All organizations in the genomic data supply chain preserve privacy and ensure that consent travels with privacy data. Privacy risks may arise even when processing data that has been aggregated or de-identified (including anonymized data). 7 - Manage reputation and trust across all organizations in the data supply chain that process genomic data. 11 - Preserve sample diversity throughout the supply chain. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders. | **1** | 2 | 2 | 2 | **1** | 2,4,5 - Identify where privacy risk to relatives or donors might arise in the genomic data processing ecosystem. Consent data will be treated as a high value and requires asset inventory and processing to know what data are subject to informed consent requirements and who can access that data. 11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations. This may be prioritized due to increased reach of data in research. The data processing environment will manage the appropriate degree of diversity.  12 - Data processing helps manage the effective, controlled sharing of genomic data across various technologies and even helps drive the requirements for technologies. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-02:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally | **1** | 2 | **1** | 2 | 2 | 1,3,6 - Enforce consistency in managing data quality, provenance, risk assessment, and access controls. 2,4,5 - Consistently communicate privacy responsibilities across the workforce, third-party stakeholders, partners, and suppliers. 8,10,12 - Coordinate consistent expectations across researchers, partners, and new technology providers for genomic data and IP protections. 9 - Laws and regulations stipulate specific cybersecurity and privacy roles and responsibilities. |
| Govern | Governance Policies, Processes, and Procedures | **PF** | **GV.PO-P3:** Roles and responsibilities for the workforce are established with respect to privacy. | 3 | 2 | 2 | 2 | 2 | 2,5,6,10 - The workforce will understand the value of the genomic data including specific privacy considerations and any relevant IP. Role-based specifics of how to manage the data life cycle will be primarily addressed in the Control and Protect functions.  9 - The workforce will clearly understand their role in pertinent legal compliance issues.  12 - New technologies will include appropriate roles to reinforce privacy requirements. |
| Govern | Governance Policies, Processes, and Procedures | **PF** | **GV.PO-P4:** Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners). | 3 | 2 | 2 | 2 | 2 | 1,4,8,12 - Coordination acts to preserve original source (provenance) and privacy rights over the life cycle and across partners. Clear expectations and roles can help address deficiencies in environments where security and privacy are not typically priorities.  2,5 - Coordination across partners will help manage privacy protections specific to donors and relatives. 9 - Legal requirements merit additional prioritization as these issues have a risk profile (reputation, compliance) and can also be difficult to define as they may cover non-technical issues. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-03:** Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes | 2 | 2 | **1** | 2 | 2 | 1 - Genomic data relies on the supply chain to maintain data quality and provenance, regularly assessing and addressing deficiencies. 2,4,5 - Privacy protections for donors and relatives are considered and assessed across the supply chain, verifying that consent travels with the data. 3 - Risk assessments address and incorporate supply chain risks to ensure protection of genomic data. 12 - Results from risk assessments of new technologies are integrated into the overall supply chain risk management process. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P2:** Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process. | **1** | 2 | **1** | 3 | **1** | 2,5 - Identify where privacy risk to relatives and donors might arise in the genomic data processing ecosystem, including re-identification.  7 - Implement external risk management activities that foster trust and are supported by all stakeholders sharing data. 11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations; manage data diversity across the ecosystem. 12 - Technologies support effective, controlled sharing of genomic data. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-04:** Suppliers are known and prioritized by criticality | **1** | 2 | 2 | 2 | 2 | 1,6,10 - Organizations prioritize suppliers who maintain data quality, provenance, access controls, and IP protections.  2,4,5 - Organizations prioritize suppliers who effectively implement privacy requirements, including managing consent. 3,7 - Risk assessments verify the trustworthiness of suppliers. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P2:** Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process. | **1** | 2 | **1** | 3 | **1** | 2,5 - Identify where privacy risk to relatives and donors might arise in the genomic data processing ecosystem, including re-identification.  7 - Implement external risk management activities that foster trust and are supported by all stakeholders sharing data. 11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations; manage data diversity across the ecosystem. 12 - Technologies support effective, controlled sharing of genomic data. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-05:** Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties | **1** | **1** | 2 | **1** | **1** | 2,4,5 - Contracts help manage and communicate privacy and consent requirements that need to travel with the data. 9 - Contracts provide the legal avenue for enforcing agreements. 12 - When contracts are used with technology suppliers, appropriate cybersecurity language will be included to enforce consistency in risk management. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P3:** Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization’s privacy program. | **1** | 2 | 2 | 2 | **1** | 4 - Contracts are a primary mechanism for establishing expectations for managing consent and ensuring that consent travels with the data. 7 - Contracts ensure that external risk management activities that foster trust are supported by stakeholders. 12 - Secure technologies track and enforce data processing requirements to implement contractual agreements. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-06:** Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships | **1** | 2 | **1** | 2 | 2 | 1,3,6,8 - Assess risks to data quality, provenance, and access control before using any genomic data organization as part of the supply chain. 2,4,5 - Determine whether suppliers implement effective privacy practices, including managing consent. 12 - Technology providers will want to assess any supplier dependencies and ensure that they are able to demonstrate their trustworthiness as a supplier. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P1:** Data processing ecosystem risk management policies, processes, and procedures are identified, established, assessed, managed, and agreed to by organizational stakeholders. | **1** | 2 | 2 | 2 | **1** | 2,4,5 - Identify where privacy risk to relatives or donors might arise in the genomic data processing ecosystem. Consent data will be treated as a high value and requires asset inventory and processing to know what data are subject to informed consent requirements and who can access that data. 11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations. This may be prioritized due to increased reach of data in research. The data processing environment will manage the appropriate degree of diversity.  12 - Data processing helps manage the effective, controlled sharing of genomic data across various technologies and even helps drive the requirements for technologies. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-07:** The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship | 2 | 2 | **1** | 2 | 2 | 2,4,5 - Monitoring can confirm that consent and other privacy requirements are managed appropriately. Monitoring may be the best way to determine any impact on relatives' privacy. 3,6,9,12 - Supplier risk assessment and ongoing monitoring address changes in threats, technologies, processes, legal or contractual requirements, and other risk factors. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P2:** Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process. | **1** | 2 | **1** | 3 | **1** | 2,5 - Identify where privacy risk to relatives and donors might arise in the genomic data processing ecosystem, including re-identification.  7 - Implement external risk management activities that foster trust and are supported by all stakeholders sharing data. 11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations; manage data diversity across the ecosystem. 12 - Technologies support effective, controlled sharing of genomic data. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P5:** Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations. | 2 | 3 | 2 | 2 | 2 | 7 - Assessments can be used as a mechanism for verifying and demonstrating trust between stakeholders. 12 - Assess technologies for effectiveness in managing privacy requirements. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-08:** Relevant suppliers and other third parties are included in incident planning, response, and recovery activities | 2 | 3 | 2 | 3 | 3 | 1,6,10 - Coordinate across partners to maintain provenance, data quality, data access, and IP protections during response and recovery operations. 2,4,5 - Plans define and communicate partners’ privacy-related response and recovery responsibilities and associated privacy requirements. 9 - Involve all appropriate parties in response and recovery to support legal requirements for processing genomic data. 12 - Organizations using new technologies determine when suppliers need to be involved in response and recovery activities. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-09:** Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle | **1** | 2 | **1** | 2 | 2 | 2,4,5 - Organizations involved in the genomic data supply chain comply with privacy and consent requirements. Privacy risks may arise even when processing data that has been aggregated or de-identified (including anonymized data). 12 - The risks introduced by suppliers of new technologies are monitored and managed throughout the product life cycle. |
| Govern | Cybersecurity Supply Chain Risk Management | **CSF** | **GV.SC-10:** Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement | 2 | **1** | 2 | 2 | **1** | 2,4,5 - If data is not appropriately protected after the agreement ends, it may impact relatives' privacy as well as donors and fail to follow consent requirements. 7,8 - Partners who fail to protect data after the agreement ends will not be trusted in the future.  12 - Supporting technologies incorporate ways to verify that there is no residual data access after use and agreements end. |
| Identify | Asset Management | **CSF** | **ID.AM-01:** Inventories of hardware managed by the organization are maintained | 2 | 3 | 2 | 3 | 2 | 1,8 - Monitor genomic data processing hardware to prevent issues with provenance or data quality. 6,12 - Hardware inventories help identify new technologies and unauthorized hardware that may be used for unauthorized access to sensitive data.  9 - Legal requirements may include maintaining an asset inventory as part of standards of practice or regulatory requirements. 10 - Protect IP information from all potential threat vectors, including hardware. |
| Identify | Inventory and Mapping | **PF** | **ID.IM-P1:** Systems/products/services that process data are inventoried. | **1** | 2 | **1** | 2 | 2 | 4 - Inventory the data to understand data types, consent requirements, and applicable regulations; inventory the systems to understand data processing across systems and how consent is shared. 8 - Data process inventories inform research data management by identifying and tracking data collection and sharing processes. |
| Identify | Inventory and Mapping | **PF** | **ID.IM-P2:** Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried. | **1** | 2 | **1** | 2 | 2 | 2 - Situational awareness of ownership helps ensure data are accessed and shared appropriately; restricting who has access may help restrict the ability to identify relatives. 3 - Roles help identify potential risks from external parties. 10 - Ownership establishes and traces provenance, who can access the IP, how to protect the IP and related business interests, and who is responsible for protecting the IP. |
| Identify | Inventory and Mapping | **PF** | **ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties). | **1** | 3 | **1** | 2 | 3 | 4 - The data processing environment may influence donors' decisions regarding consent. For example, they may accept data processing in their home country but not in locations with differing privacy standards, or they may be comfortable with data being processed in-house but uncomfortable with data being processed in a cloud environment.  9 - International data sovereignty and privacy rights may impose unique challenges that require stricter compliance with laws and regulations; location determines applicable laws, regulations, policies, and standards. |
| Identify | Asset Management | **CSF** | **ID.AM-02:** Inventories of software, services, and systems managed by the organization are maintained | **1** | 2 | **1** | 2 | 2 | 1,3,6 - Software and services represent a primary attack vector for unauthorized access and data breaches. 2,5 - Inventories are used to identify potential harms from software used to process relatives’ and donors’ data. 10 - Inventories of software interacting with IP or of the IP itself provide an awareness of potential attack vectors. 12 - Software and systems delivered as part of new technologies represent a significant risk. |
| Identify | Inventory and Mapping | **PF** | **ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties). | **1** | 3 | **1** | 2 | 3 | 4 - The data processing environment may influence donors' decisions regarding consent. For example, they may accept data processing in their home country but not in locations with differing privacy standards; or they may be comfortable with data being processed in-house but uncomfortable with data being processed in a cloud environment.  9 - International data sovereignty and privacy rights may impose unique challenges that require stricter compliance with laws and regulations; location determines applicable laws, regulations, policies, and standards. |
| Identify | Inventory and Mapping | **PF** | **ID.IM-P1:** Systems/products/services that process data are inventoried. | **1** | 2 | **1** | 2 | 2 | 4 - Inventory the data to understand data types, consent requirements, and applicable regulations; inventory the systems to understand data processing across systems and how consent is shared. 8 - Data process inventories inform research data management by identifying and tracking data collection and sharing processes. |
| Identify | Asset Management | **CSF** | **ID.AM-03:** Representations of the organization's authorized network communication and internal and external network data flows are maintained | **1** | **1** | 2 | **1** | **1** | 1,6,8 - Network communications and data flows help track where and how genomic data is being used, along with any impact on data quality, provenance, and access throughout the genomic data life cycle. 2,4,5 - Organizations track where donors’ and relatives’ data are processed to manage privacy requirements, including consent, which travels with the data.  10 - Mapping data flows can help identify threats to IP everywhere it is processed. 12 - Tracking data flows for new technologies integrated with genomic processing helps determine where risks to data might be introduced. |
| Identify | Inventory and Mapping | **PF** | **ID.IM-P8:** Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services. | **1** | 2 | **1** | 2 | 2 | 2,4,5 - Privacy risk directly correlates to data processing and cannot be evaluated without understanding the data actions and data flows. Informed consent means understanding data processing activities and locations, privacy and security protections, and what consent will mean for the donor. 9 - Data processing inventories support compliance with laws and regulations, understanding what schemas apply (e.g., GDPR, HIPAA), and understanding citizenship for data subjects (e.g., GDPR, state laws).  12 - Technologies may help bring people to the data rather than sharing the data across multiple internal and external environments. Manage the inventory across the range of technologies and environments: cloud, private networks, locations, etc. |
| Identify | Asset Management | **CSF** | **ID.AM-04:** Inventories of services provided by suppliers are maintained | **1** | 2 | 2 | 2 | 2 | 1,3,6,12 - Genomic data processing is becoming increasingly more complex and interconnected (e.g., genomic data banks and research initiatives). Service inventories help identify potential risk sources introduced by suppliers. 4 - Inventorying services helps manage consent, which travels with human genomic data. 8 - Service inventories help research institutions understand how data may be impacted by other services in data analysis pipelines. 10 - IP in the form of software or data may be a high-value target and is at risk from unauthorized or shadow services associated with third-party suppliers. |
| Identify | Inventory and Mapping | **PF** | **ID.IM-P2:** Owners or operators (e.g., the organization or third parties such as service providers, partners, customers, and developers) and their roles with respect to the systems/products/services and components (e.g., internal or external) that process data are inventoried. | **1** | 2 | **1** | 2 | 2 | 2 - Situational awareness of ownership helps ensure data are accessed and shared appropriately; restricting who has access may help restrict the ability to identify relatives. 3 - Roles help identify potential risks from external parties. 10 - Ownership establishes and traces provenance, who can access the IP, how to protect the IP and related business interests, and who is responsible for protecting the IP. |
| Identify | Inventory and Mapping | **PF** | **ID.IM-P7:** The data processing environment is identified (e.g., geographic location, internal, cloud, third parties). | **1** | 3 | **1** | 2 | 3 | 4 - The data processing environment may influence donors' decisions regarding consent. For example, they may accept data processing in their home country but not in locations with differing privacy standards; or they may be comfortable with data being processed in-house but uncomfortable with data being processed in a cloud environment.  9 - International data sovereignty and privacy rights may impose unique challenges that require stricter compliance with laws and regulations; location determines applicable laws, regulations, policies, and standards. |
| Identify | Asset Management | **CSF** | **ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and impact on the mission | **1** | 2 | **1** | 2 | 2 | 1,6 - Data prioritization and classification are inherently part of managing data provenance, integrity, and access control activities. 2,5 - Organizations prioritize privacy attributes when determining the value of genomic data (in addition to business- and mission-related values). 9 - Legal requirements vary across geographies and require comprehensive classification efforts. 10 - For genomic research, the IP may be the data itself (or derivatives of its use). |
| Identify | Asset Management | **CSF** | **ID.AM-07:** Inventories of data and corresponding metadata for designated data types are maintained | **1** | **1** | **1** | **1** | **1** | 1 - Data provenance management requires maintaining data and metadata inventories. 2,5 - Metadata helps identify security and privacy concerns for relatives and donor data where risks or harms can occur from secondary associations. 4 - Consent in the form of either data or metadata will be inventoried and associated with its respective genomic information at all stages of processing. 6 - Access control is dependent on knowing the type, classification, and location of data throughout its life cycle in the ecosystem. 8,9,10 - Understanding the types of data processed drives cybersecurity and legal protections in research environments, for privacy data, and for IP. |
| Identify | Inventory and Mapping | **PF** | **ID.IM-P6:** Data elements within the data actions are inventoried. | **1** | 2 | **1** | 2 | 2 | 2,4,5 - Privacy risk directly correlates to data processing and cannot be evaluated without understanding the data elements, which may contain information pertaining to relatives, donors, and consent. Consent practices can be managed at the data element level when necessary. 8 - Data management is part of managing research. Research activities may have increased or specialized data handling requirements. 11 - Data elements may determine the degree of diversity (i.e., do you have enough data to make a determination?) and provide statistical confidence. Genomic sample diversity enables researchers to identify genetic variants with greater statistical confidence, and allows for a more comprehensive and inclusive understanding of diverse populations. |
| Identify | Asset Management | **CSF** | **ID.AM-08:** Systems, hardware, software, services, and data are managed throughout their life cycles | **1** | **1** | 2 | **1** | **1** | 1 - Data quality and provenance depend on managing systems and data across the entire life cycle. 2,4, 5 - Cybersecurity privacy considerations span the entire data life cycle, including acquiring, aggregating, and disposing of data according to consent and other privacy requirements. 3,9 - Implementing life cycle processes and activities helps manage and address the risks associated with processing genomic data while also reflecting laws or guidance that stipulate patching outdated software or migration away from unsupported hardware and software. 6 - Managing systems includes identifying redundant or non-compliant systems that may expose systems or data to unauthorized access. 8 - Research environments often include outdated assets that may require compensating controls to protect the data. 10 - IP protections will be confirmed throughout the life cycle to prevent unauthorized tampering or disclosure during system development, upgrade, migration, or disposal. |
| Protect | Maintenance | **PF** | **PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. | 2 | 3 | 3 | 3 | 3 | 1,4,5,6,10 - Logging maintenance and repairs impacts an organization’s ability to manage data, protect IP, and maintain quality, using audits of such activities to establish and trace data ownership and provenance. Logging also supports tracking who accessed privacy data to manage consent. |
| Protect | Maintenance | **PF** | **PR.MA-P2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. | 2 | 3 | 3 | 3 | 3 | 1,4,9 - Access (whether authorized or unauthorized) as part of remote maintenance to devices and machines needs to be controlled to prevent people from accessing, modifying, or deleting sensitive information and support appropriate use of data consistent with consent or legal/regulatory compliance. |
| Control | Data Processing Management | **PF** | **CT.DM-P5:** Data are destroyed according to policy. | **1** | **1** | 2 | 2 | **1** | 2 - Data destruction limits the long-term ability to infer associations with relatives.  4,5,7 - Implement consent and foster donor trust by deleting data in accordance with individual preferences and the relevant retention schedule. 6 - Deletion in accordance with retention policies supports restricting unauthorized access.  11 - Failure to delete data impacts trust in under-represented populations and makes it less likely that a diverse group of donors will participate. |
| Control | Data Processing Policies, Processes, and Procedures | **PF** | **CT.PO-P4:** A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems. | **1** | 2 | 2 | 2 | 2 | 1, 3 - Data and system life cycles integrate risk management processes and protect data quality and provenance. 4,12 - Consent will be managed throughout data and system life cycles, with special care to address data aggregation and possible re-assessment when technologies enable new processing capabilities and privacy engineering practices. 9 - Governance and regulatory compliance may focus on an organization’s ability to manage data and system life cycles. |
| Protect | Data Security | **PF** | **PR.DS-P3:** Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition. | **1** | 2 | 2 | 3 | **1** | 1,10,12 - This helps establish and trace data and IP ownership and provenance to manage data throughout its life cycle. 8 - Security to protect against data leaks is needed at all steps in research, from device to data storage. Too often, sunset datasets are left unprotected and sunset equipment is disposed of without removing stored data. As more researchers gain access to genomic data, enhanced or additional protections may be required. 9 - Organizations will comply with legal and regulatory requirements for destruction and proper disposal. 12 - Organizations implementing new technologies manage both the disposal of old devices and the acquisition of any new devices to protect the data. |
| Identify | Risk Assessment | **CSF** | **ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded | **1** | 2 | **1** | 3 | 2 | 1,6 - Data provenance, integrity, and access protections begin with identifying and addressing system vulnerabilities that might compromise genomic data throughout its life cycle. 2,5 - Vulnerability assessment reduces potential harms to donors and relatives by protecting their data from threats such as unauthorized access or data breaches. 3,8,10,12 - Vulnerability management provides a baseline for managing risks to genomic data that will be applied in research environments, when protecting IP, and for assessing risks from new technologies. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P10:** A vulnerability management plan is developed and implemented. | 2 | 3 | **1** | 3 | 3 | 3 - These plans provide the vulnerability inputs to risk modeling and management.  4,5 - Vulnerabilities may directly impact privacy and consent and will be tracked comprehensively to manage associated risks. 12 - The plan will include provisions for how to manage vulnerabilities introduced in new technologies and ensure that contracts with technology providers incorporate sufficient support to ensure remediation of vulnerabilities throughout the technology life cycle. |
| Identify | Risk Assessment | **CSF** | **ID.RA-02:** Cyber threat intelligence is received from information sharing forums and sources | 3 | 3 | **1** | 3 | 3 | 3 - CTI provides the threat input to risk modeling and management. 7 - Receiving and sharing CTI as part of a common effort to address threats collectively can build trust among genomic community participants. 10,12 - Monitoring CTI can provide an organization with insight into potential threats to its IP or new technologies. |
| Identify | Risk Assessment | **CSF** | **ID.RA-03:** Internal and external threats to the organization are identified and recorded | **1** | 2 | **1** | 3 | 2 | 1,3,10 - Maintaining awareness of likely threat actors targeting the organization informs effective practices for risk reduction and protection of high-value assets (such as genomic data and related IP). 7,9 - The consistent use of CTI demonstrates a level of due diligence and adherence to legal requirements that benefits the organization’s reputation in the event of cyberattacks or data breaches. 8,12 - The use of the emerging and rapidly evolving technology typically found in research requires vigilant identification of new threats and tactics, techniques, and protocols (TTPs). |
| Identify | Risk Assessment | **PF** | **ID.RA-P3:** Potential problematic data actions and associated problems are identified. | **1** | **1** | **1** | 2 | **1** | 2,4,5 - PDAs may include combining data sources that could create privacy harms impacting donors and/or relatives and violate informed consent. 10 - Evaluate the impact on IP from PDAs, including those introduced by open-source software. 11 - Diversity is not just in collection. Changes in the data through processing may affect the ability to maintain data diversity. Specific populations or individuals can have differing views on data processing and what constitutes a PDA. 12 - Technologies may play a role in managing risk from PDAs related to data sharing. Use of technology may also introduce PDAs and associated risks. |
| Identify | Risk Assessment | **CSF** | **ID.RA-04:** Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded | 2 | 2 | **1** | 2 | 2 | 1,2,5 - The potential impacts of exploited vulnerabilities can impact the organization as well as donors and relatives, since genomic data is a unique identifier. By identifying and understanding the potential impact on the organization and individuals, organizations can assess the likelihood and impact of risk scenarios. 3 - Likelihood and impacts serve as inputs in modeling and managing risks. 8,12 - External stakeholders involved in broader research and data-sharing initiatives will be considered when identifying potential impacts, including those introduced through new technologies. |
| Identify | Risk Assessment | **PF** | **ID.RA-P4:** Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk. | 2 | **1** | **1** | 2 | **1** | 2,4,5 - If PDAs impact consent or the privacy of donors or relatives, that risk will be assessed and managed, considering secondary risks (e.g., to relatives or downstream in managing consent). 8 - Understand the impact on the research, including research environment, data, and outcomes. 9 - Monitor the PDAs’ impact on legal requirements.  12 - Assess PDAs to identify concerns with data processing activities, use of technologies, and data-sharing activities. |
| Identify | Risk Assessment | **CSF** | **ID.RA-05:** Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization | **1** | **1** | **1** | 2 | **1** | 1,3,10 - Organizations prioritize resource allocations and risk responses for high-value assets (particularly genomic data and IP) based on risk models that are developed from these inputs. 2,4,5 - Inherent risk from potential privacy harms to relatives and donors is considered as part of the risk equation. 8,12 - Threats and impacts to the organization and stakeholders from data-sharing agreements and new technologies are inputs for inherent risk determination. |
| Identify | Risk Assessment | **PF** | **ID.RA-P4:** Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk. | 2 | **1** | **1** | 2 | **1** | 2,4,5 - If PDAs impact consent or the privacy of donors or relatives, that risk will be assessed and managed, considering secondary risks (e.g., to relatives or downstream in managing consent). 8 - Understand the impact to the research including research environment, data, and outcomes. 9 - Monitor the PDAs’ impact on legal requirements.  12 - Assess PDAs to identify concerns with data processing activities, use of technologies, and data sharing activities. |
| Identify | Risk Assessment | **CSF** | **ID.RA-06:** Risk responses are chosen, prioritized, planned, tracked, and communicated | **1** | 2 | **1** | 3 | 2 | 1 - Risk response planning helps coordinate the activities required (internal and external) to manage data quality and provenance when events occur. 2,4,5 - Cybersecurity-related risk responses for privacy harms to donors and relatives are understood, documented, and prioritized. 8 - Due to the broadness of the research community, researchers consider the entire ecosystem when developing effective risk responses. 9 - Risk responses consider any legally-required response activities, including tracking progress of such activities and data breach notification. 10 - Risk responses will ensure that appropriate protections are in place for IP. |
| Identify | Risk Assessment | **PF** | **ID.RA-P5:** Risk responses are identified, prioritized, and implemented. | 2 | 2 | **1** | 3 | 2 | 2,4,5 - Response includes appropriate notification when consent or privacy of donors or relatives is impacted.  12 - Use of technologies will document potential issues that need to be evaluated during response and recovery operations. Notification of technology providers and consumers will be prioritized. |
| Identify | Risk Assessment | **CSF** | **ID.RA-07:** Changes and exceptions are managed, assessed for risk impact, recorded, and tracked | **1** | 2 | 2 | 2 | 2 | 1 - Risks to data quality and provenance will evolve and will be tracked and periodically reviewed for security implications. 2,4,5 - Changes in risk determinants related to privacy harms require formal review, testing, and approvals to remain relevant and effective. 6 - Reviewing changes in configuration profiles and protections supports organizational change management needed for access control requirements. 9 - Organizations monitor changes to laws and regulations to determine cybersecurity impacts. 10 - Organizations monitor the impact of changes that may affect or introduce risks to IP. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P2:** Configuration change control processes are established and in place. | **1** | 3 | 2 | 3 | 2 | 1,3,6 - Change control reduces the risk of unauthorized changes that may impact data access, quality, or provenance and ensures that risks from new changes are evaluated. 2,4,5 - Change control will monitor for changes that may impact the effectiveness of privacy controls and the ability to manage consent.  12 - Change control for new technologies will be used to ensure unauthorized changes don’t occur that introduce additional privacy or security risks. |
| Identify | Risk Assessment | **CSF** | **ID.RA-08:** Processes for receiving, analyzing, and responding to vulnerability disclosures are established | 2 | 2 | 2 | 3 | 2 | 1,10 - Organizations protecting data quality, provenance, and IP will want to quickly address identified system vulnerabilities. 3 - Effective risk management involves consistently managing vulnerability disclosures and implementing appropriate protections. 8,11,12 - Environments with broad attack surfaces, emerging technologies, or multiple stakeholders will benefit the most from coordinated response to vulnerabilities by external sources. |
| Identify | Risk Assessment | **CSF** | **ID.RA-09:** The authenticity and integrity of hardware and software are assessed prior to acquisition and use | 2 | 3 | 3 | 3 | 3 | 1 - Hardware and software require authenticity testing to identify tampered assets that may threaten data quality or provenance. 2,4,5 - Systems may be tampered with to attempt unauthorized access to privacy-related information. 8,12 - Research and new technologies may include a wide range of equipment, proprietary hardware, and IoT devices. Testing assures that minimum acceptance criteria are met. 10 - Testing of hardware and software prior to use can identify potential vulnerabilities (e.g., malicious code, backdoors) that can be exploited for attacks on IP. |
| Protect | Data Security | **PF** | **PR.DS-P8:** Integrity checking mechanisms are used to verify hardware integrity. | 2 | 3 | 2 | 3 | 3 | 1 - Integrity checking for hardware may be prioritized to manage data quality and chain of provenance. 12 - Emerging technologies may use integrity-checking mechanisms and ensure that hardware devices are from approved sources, noting that laws may ban the use of hardware from certain nation states. |
| Identify | Risk Assessment | **CSF** | **ID.RA-10:** Critical suppliers are assessed prior to acquisition | **1** | 2 | **1** | 2 | 2 | 1,2,4,5 - Supplier risk assessments help identify problematic assets or services including any risks to data quality, provenance, consent, and donors’ or relatives’ privacy. 7 - Obtaining unsecured, counterfeit, or unauthentic supplies puts the organization's trustworthiness and reputation at risk. 12 - New technologies may include hardware and software from third-party suppliers that will be assessed prior to acquisition, particularly when they are produced by a supplier in a location of concern. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P2:** Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process. | **1** | 2 | **1** | 3 | **1** | 2,5 - Identify where privacy risk to relatives and donors might arise in the genomic data processing ecosystem, including re-identification.  7 - Implement external risk management activities that foster trust and are supported by all stakeholders sharing data. 11 - Prevent unwanted identifiability of individuals, especially those in vulnerable sub-populations; manage data diversity across the ecosystem. 12 - Technologies support effective, controlled sharing of genomic data. |
| Identify | Data Processing Ecosystem Risk Management | **PF** | **ID.DE-P5:** Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual, interoperability framework, or other obligations. | 2 | 3 | 2 | 2 | 2 | 7 - Assessments can be used as a mechanism for verifying and demonstrating trust between stakeholders. 12 - Assess technologies for effectiveness in managing privacy requirements. |
| Identify | Improvement | **CSF** | **ID.IM-01:** Improvements are identified from evaluations | 3 | 2 | **1** | 3 | 2 | 2,5 - Assessments identify how well protections perform in safeguarding donors’ and relatives’ data, and provide input for continued effectiveness against updated threats and TTPs. 3 - Risk analysis is a point-in-time evaluation, so continuous assessment and evaluation is needed to provide a dynamic understanding of risk. 10 - Highly valued IP assets require ongoing protections and benefit from the continuous improvements identified through ongoing risk and controls evaluation. 12 - New technologies will be continuously assessed to identify needs for improvement. |
| Identify | Improvement | **CSF** | **ID.IM-02:** Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties | 2 | 2 | 2 | 3 | 2 | 1 - Testing across the data life cycle discovers opportunities to improve protections to data quality and provenance, especially in data-sharing arrangements with third parties having different security postures. 7 - Testing exercises among partners and suppliers validate protections and promote trust between partners. 10 - Security test results can identify opportunities to improve the security posture of IP protections, including resilience and business continuity (for example, in the case of ransomware). |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P8:** Response and recovery plans are tested. | 2 | 2 | 2 | 3 | 2 | 2,5 - Testing plans ensures that response and recovery activities are effective to limit the privacy impact of an incident and recover to an acceptable state. 8,12 - When new technologies are introduced, there may be special needs for response and recovery to ensure that teams understand any new requirements. Additionally, testing helps ensure that response and recovery across partners are effective. |
| Identify | Improvement | **CSF** | **ID.IM-03:** Improvements are identified from execution of operational processes, procedures, and activities | 2 | 2 | 2 | 3 | 2 | 8 - Organizations conduct lessons-learned activities among research partners to identify gaps and attain minimum baseline protections that support reproducibility in research. 10 - Organizations improve IP protections, monitoring operations to identify security gaps and proactively fortify against future threats. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P5:** Protection processes are improved. | 3 | 3 | 3 | 3 | 3 | 1 - Protection processes can include assurances that data are appropriate for processing purposes and that the chain of provenance remains intact. 2,4,5,8,12 - Specific PETs may require new processes to achieve the benefits, including data minimization, encryption, or de-identification. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P6:** Effectiveness of protection technologies is shared. | 2 | 3 | 3 | 3 | 3 | 2,4,5,9 - Sharing across the ecosystem ensures that any issues impacting donors’ or relatives’ privacy are appropriately communicated in accordance with laws and policy.  6,8,12 - Researchers and technology providers will want to share any issues with data protections to ensure rapid remediation across the entire ecosystem and minimize the impact of unauthorized data access.  7 - Communication builds and maintains trust across partners. |
| Identify | Improvement | **CSF** | **ID.IM-04:** Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved | 2 | 2 | **1** | 3 | 2 | 2,4,5 - Contingency plans include relevant information on processes for communicating with donors and relatives to inform them of privacy harms and adverse events (such as data breaches). 3 - Risk modeling identifies areas that require incident response activities to be included in the response plans. 7 - Maintaining contingency plans demonstrates due diligence and trustworthiness in managing cybersecurity risks. 10 - Plans will ensure that IP is protected when cybersecurity events occur, supporting the continuity of the organization’s mission and viability. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P7:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | 2 | 3 | 2 | 3 | 2 | 2,4,5,9 - Response plans will include appropriate actions to identify, manage, and recover from privacy breaches, including notifying donors, returning to an acceptable state in accordance with consent agreements, and complying with legal and contractual requirements. 3 - Risk management strategies will include appropriate response planning and processes including managing any adverse outcomes for the individuals affected. 7 - Response and recovery activities will directly impact an organization’s reputation and the trust of partners who rely on the organization.  10 - Response and recovery plans identify any IP to protect and recover it so that IP data is available to be used for business purposes. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P8:** Response and recovery plans are tested. | 2 | 2 | 2 | 3 | 2 | 2,5 - Testing plans ensures that response and recovery activities are effective to limit the privacy impact of an incident and recover to an acceptable state. 8,12 - When new technologies are introduced, there may be special needs for response and recovery to ensure that teams understand any new requirements. Additionally, testing helps ensure that response and recovery across partners are effective. |
| Protect | Identity Management, Authentication, and Access Control | **CSF** | **PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization | **1** | **1** | **1** | **1** | **1** | 1,6,10 - Robust identity and credential management enables an organization to manage access to genomic data throughout the life cycle and enforce accountability for data quality, provenance, and IP protections. 2,4,5 - Privacy protections require the ability to manage who accesses data and what they do with the data. This may be especially important for high-value data that can be used to link individuals. 8,12 - Shared environments and new technologies integrate identity and credential management to authenticate and authorize users, services, and assets. |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | **1** | 3 | 2 | 2 | 2 | 1,4,6 - Identity (of person, service, app, etc.) is used to monitor and manage data access to support data access, quality, provenance, and consent requirements. Consent travels with the data, with access managed at the identity level.  3,5 - Controlling access supports managing privacy risk by reducing exposure of data and the potential privacy harms due to genetic association/combining data sources that may result in data being identified/re-identified. 7,8,12 - Compromised identity will destroy trust, including trust between partners, even when using privacy-preserving technologies. Legacy and new technologies will both support consistent identity management. |
| Protect | Identity Management, Authentication, and Access Control | **CSF** | **PR.AA-02:** Identities are proofed and bound to credentials based on the context of interactions | 2 | 3 | 2 | 3 | 3 | 1,3 - For high-value data, identity proofing enables organizations to implement more granular access controls in support of data quality and provenance. 6 - This capability will help organizations implement granular access control as part of a zero-trust architecture. 2,4,5,10 - These capabilities enhance sensitive data protections, aligned with efforts to implement other requirements related to a zero-trust architecture. |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P6:** Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks). | 2 | 3 | 2 | 2 | 2 | 1,6,8,9,10,12 - This level of granularity can be used to help manage data quality and provenance, research environment integrity, trust, reputation, legal and regulatory requirements, IP protection, and new technologies. 2,4,5 - Authentication commensurate with the risk of the transaction helps to implement additional privacy controls that protect consent based on the privacy risk. |
| Protect | Identity Management, Authentication, and Access Control | **CSF** | **PR.AA-03:** Users, services, and hardware are authenticated | **1** | **1** | 2 | 2 | **1** | 1,2,4,5,10 - Authentication capabilities will be prioritized to enhance data quality, provenance, and access protections for privacy data and IP. 3,8,12 - Whenever data is shared or new technology is integrated, managing authentication, including remote access capabilities, helps control data access and reduce the risk of data corruption or loss. |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P3:** Remote access is managed | 2 | 3 | 2 | 2 | 2 | 1,9 - Some organizations may decide to manage remote access in a way that will prohibit local downloading of data (e.g., biobanks, commercial terms) to comply with legal /regulatory requirements around downloading. 2,4,5 - Remote access across partners will implement consistent, appropriate privacy protections according to consent requirements. 6,8 - All forms of remote access, including vendor updates and maintenance and access to research environments, will be managed. 12 - Technologies bring people to data via remote access. Authorized individuals need access to effective, controlled data-sharing capabilities. Adopting zero-trust principles remains relevant in this case, especially with the increased practice of using remote access [e.g., the 21st Century Cures Act allows remote access to personally identifiable information (PII) in research [20].] |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P6:** Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks). | 2 | 3 | 2 | 2 | 2 | 1,6,8,9,10,12 - This level of granularity can be used to help manage data quality and provenance, research environment integrity, trust, reputation, legal and regulatory requirements, IP protection, and new technologies. 2,4,5 - Authentication commensurate with the risk of the transaction helps to implement additional privacy controls that protect consent based on the privacy risk. |
| Protect | Identity Management, Authentication, and Access Control | **CSF** | **PR.AA-04:** Identity assertions are protected, conveyed, and verified | 2 | 2 | 3 | 3 | 2 | 1,3 - Verifying identity assertions can improve risk management and data protections by preventing unauthorized access. 2, 5, 6, 8, 10, 12 - Identity assertions support an organization’s ability to manage access and prevent unauthorized access (e.g., by third parties, research partners, remote users). |
| Protect | Identity Management, Authentication, and Access Control | **CSF** | **PR.AA-05:** Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties | **1** | **1** | 2 | 2 | **1** | 1,3,6,10 - These capabilities prevent issues with data quality, provenance, access, and sharing.  2,4,5 - Privacy protections rely on appropriate access management through least privilege, separation of duties, and role-based access control (or other more restrictive means) to manage who accesses data and what they do with the data.  8 - Researchers and their partners proactively manage authorizations in environments where there is high turnover, fewer physical access controls, or a greater need to protect sensitive data. |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices. | **1** | 3 | 2 | 2 | 2 | 1,4,6 - Identity (of person, service, app, etc.) is used to monitor and manage data access to support data access, quality, provenance, and consent requirements. Consent travels with the data, with access managed at the identity level.  3,5 - Controlling access supports managing privacy risk by reducing exposure of data, reducing the potential privacy harms due to genetic association/combining data sources that may result in data being identified/re-identified. 7,8,12 - Compromised identity will destroy trust, including trust between partners, even when using privacy-preserving technologies. Legacy and new technologies will both support consistent identity management. |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P3**: Remote access is managed | 2 | 3 | 2 | 2 | 2 | 1,9 - Some organizations may decide to manage remote access in a way that will prohibit local downloading of data (e.g., biobanks, commercial terms) to comply with legal /regulatory requirements around downloading. 2,4,5 - Remote access across partners will implement consistent, appropriate privacy protections according to consent requirements. 6,8 - All forms of remote access, including vendor updates and maintenance and access to research environments, will be managed. 12 - Technologies bring people to data via remote access. Authorized individuals need access to effective, controlled data sharing capabilities. Adopting zero trust principles remains relevant in this case, especially with the increased practice of using remote access [e.g., 21st Century Cures Act allows remote access to personally identifiable information (PII) in research [20].] |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. | **1** | 2 | 2 | 2 | 2 | 2,4,5 - Access controls determine who can do what with the data (via authentication and authorization), enabling consent management and protecting against loss or unauthorized access to donor or relative information. 3,8,9,10,12 - Risk assessment will evaluate and prioritize access controls to ensure privacy, protect IP, and comply with laws and regulations, particularly focusing on data-sharing partnerships. |
| Protect | Identity Management, Authentication, and Access Control | **CSF** | **PR.AA-06:** Physical access to assets is managed, monitored, and enforced commensurate with risk | 3 | 2 | 3 | 3 | 2 | 3,6 - Physical access risks are included in risk models along with access protections applying to physical environments. 8 - Organizations operating physical data-sharing environments may assign a higher priority to managing physical access. |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P2:** Physical access to data and devices is managed. | 2 | 3 | 3 | 3 | 3 | 1,6,8 - Physical access may not be the typical access vector, but organizations will manage who has physical access to data and devices to manage data quality and provenance across partners. Physical access to wet labs will also be managed. 10 - Access to IP will be managed consistent with any legal restrictions. Data owners and custodians will understand what they can access and how it can be used. |
| Protect | Protective Technology | **PF** | **PR.PT-P3:** Communications and control networks are protected. | 2 | 3 | 3 | 3 | 3 | 1,12 - This may be relevant to data storage and analysis needs within an organization or when using emerging technologies for transferring data. 8 - Protecting research networks may require technical security solutions that can help with wider data sharing with the research community. |
| Protect | Awareness and Training | **CSF** | **PR.AT-01:** Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind | 2 | **1** | 2 | **1** | **1** | 2,4,5 - Training includes privacy-related topics (e.g., personnel knowing what to do if they come across genomic data they shouldn’t have access to). Training for suppliers and partners includes privacy requirements such as ensuring that consent travels with the data.  6 - Training helps enforce the same data access requirements across all parties. 7 - Organizations train users on how to manage reputational risks. 8,12 - Personnel in data-sharing environments are trained to understand their roles and responsibilities, including training on new technologies. 9 - Training helps maintain legal and regulatory compliance.  10 - Organizations with IP will ensure that those with access to IP understand how to protect it. 11 - Third parties who provide samples will understand the requirements for sample diversity. |
| Govern | Awareness and Training | **PF** | **GV.AT-P1:** The workforce is informed and trained on its roles and responsibilities. | **1** | 2 | 2 | 2 | 2 | 6 - Access controls among the various data roles (owners, stewards, users, custodians, processors) are generally recognized as a high priority, preventative technical control.  8 - Researchers need to manage the privacy protection issues introduced by high turnover in the workforce that is common in universities and other similar settings. 12 - Users from various organizations will have specialized training on technologies used by a research consortium. |
| Protect | Awareness and Training | **CSF** | **PR.AT-02:** Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind | 2 | **1** | 2 | 2 | **1** | 2,4,5 - Specialized training equips personnel to recognize sensitive data and relevant privacy, legal, regulatory, and compliance constraints. 6 - Training helps implement the same data access requirements across all parties. 7,9 - Senior executives are the primary personnel responsible for managing risks to reputation and trust as well as legal compliance. 8,12 - In shared processing environments, personnel in specialized roles implement and ensure that appropriate protections are in place, including personnel screening. Privileged users with access to shared data environments have a higher responsibility to protect the data and the environment. 10 - Senior executives and other privileged users are responsible for protecting IP. 11 - Third parties who provide samples understand requirements for sample diversity. |
| Govern | Awareness and Training | **PF** | **GV.AT-P2:** Senior executives understand their roles and responsibilities. | 2 | 3 | 2 | 2 | 2 | 2,4,5,7,8,11,12 - Leadership prioritizes awareness and training efforts and provides the resources to support implementation. Executives may also include Chief Privacy Officers.  9 - Senior executives will need to make a risk-based judgment call in cases where they cannot meet compliance obligations. They also need to be aware of local and international legal and regulatory compliance requirements. |
| Govern | Awareness and Training | **PF** | **GV.AT-P3:** Privacy personnel understand their roles and responsibilities. | 2 | 2 | 2 | **1** | **1** | 5 - Privacy personnel will align their priorities among the other mission-critical and operational priorities, since they are not always in a position to know and understand all details of mission and operations.  6 - Privacy professionals will integrate with security teams and advise on the implications of providing ‘who’ access to ‘what’, which will likely be based on predetermined rules.  8 - Research enterprises generally lack resources and expertise on privacy matters, so input from privacy professionals on many aspects of privacy will be required (e.g., HIPAA).  12 - The workforce will require training on the privacy implications of any new technology. |
| Govern | Awareness and Training | **PF** | **GV.AT-P4:** Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities. | 2 | 2 | 2 | 2 | 2 | 4 - Consent will be consistently implemented across all organizations handling the data.  6,8,9,12 - Training and awareness will specify data-sharing requirements, how data access is managed, legal and regulatory requirements, and the risks from using newer technologies.  11 - Aligning to data diversity requirements among organizations with differing priorities will require a high degree of coordination. |
| Protect | Data Security | **CSF** | **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected | **1** | **1** | 2 | **1** | **1** | 2,4,5,6,10 - Data protections, including encryption, prevent unauthorized access to sensitive data and can help prevent data leaks and data breaches. 7 - Lack of safeguards (or even the perception of the lack of such implemented safeguards) can impact trust and reputation. 8,12 - Data protections including encryption help manage sensitive data at rest for every partner. New technologies support future encryption and other protection technologies. |
| Protect | Data Security | **PF** | **PR.DS-P1:** Data-at-rest are protected. | **1** | 2 | **1** | 2 | **1** | 1,6,10 - Encrypting data at rest protects stored data from unauthorized access, supporting data integrity and provenance, and protecting against leaks and breaches.  2,4,5 - Data-at-rest protections keep data secure but accessible by appropriate individuals in accordance with consent. 7,9 - Consistently applied practices such as encryption demonstrate that an organization can be trusted with data and support compliance with legal and regulatory requirements and international standards for controlling access. 12 - Organizations ensure that new technologies support encryption requirements. |
| Protect | Data Security | **PF** | **PR.DS-P5:** Protections against data leaks are implemented. | 2 | **1** | 2 | 2 | **1** | 2,3,4,5,7 - Organizations identify where privacy risks to donors and relatives might arise from data leaks and implement protections commensurate with their risk strategy to comply with consent requirements.  8 - Researchers ensure that all partners implement appropriate protections from device to data storage. Too often, sunset datasets are left unprotected and sunset equipment is disposed of without removing stored data.  12 - Organizations ensure that new technologies provide adequate protections against data leaks. |
| Protect | Data Security | **PF** | **PR.DS-P6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity. | 2 | 3 | 2 | 3 | 3 | 1,6,12 - Integrity checking enforces consistent security practices that manage provenance, ensure data quality, and restrict access. These integrity-checking mechanisms are necessary for PETs testing and verification and could be helpful for emerging technologies. |
| Protect | Protective Technology | **PF** | **PR.PT-P1:** Removable media is protected and its use restricted according to policy. | 2 | 3 | 3 | 3 | 3 | 1,4,7 - When removable media is used, policies will help protect the media and the data’s provenance, preventing data leaks and unauthorized use. 8 - Use of removable media introduces risks in protecting data when sharing among research partners. Enhanced or additional protections may be required as more researchers and partners gain access to genomic data. Organizations may need to limit use of removable media due to increased risk of loss and theft and because of other information beyond the genome. |
| Protect | Data Security | **CSF** | **PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected | **1** | **1** | 2 | **1** | **1** | 2,4,5,6,10 - Data protections, including encryption, prevent unauthorized access to sensitive data and can help prevent data leaks and data breaches. 7 - Lack of safeguards (or even the perception of the lack of such implemented safeguards) can impact trust and reputation. 8,12 - Data protections, including encryption, help manage sensitive data in transit in data-sharing environments. New technologies support future encryption and other protection technologies. |
| Protect | Data Security | **PF** | **PR.DS-P2:** Data-in-transit are protected. | **1** | 2 | **1** | 2 | **1** | 2,4,5 - Encrypting data in transit keeps data secure but also accessible by appropriate individuals in accordance with consent. 7,9 - Consistently applied practices such as encryption demonstrate that an organization can be trusted with data and support compliance with legal and regulatory requirements and international standards for controlling access. 8 - As more researchers gain access to genomic data, enhanced or additional protections may be required, such as data-in-transit protections. 12 - Organizations ensure that new technologies support encryption requirements. |
| Protect | Data Security | **PF** | **PR.DS-P5:** Protections against data leaks are implemented. | 2 | **1** | 2 | 2 | **1** | 2,3,4,5,7 - Organizations identify where privacy risk to donors and relatives might arise from data leaks and implement protections commensurate with their risk strategy to comply with consent requirements.  8 - Researchers ensure that all partners implement appropriate protections from device to data storage. Too often, sunset datasets are left unprotected and sunset equipment is disposed of without removing stored data.  12 - Organizations ensure that new technologies provide adequate protections against data leaks. |
| Protect | Data Security | **CSF** | **PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected | **1** | **1** | 2 | **1** | **1** | 2,4,5,6,10 - Measures to prevent unauthorized access to sensitive data-in-use can help prevent data leaks and data breaches.  7 - Lack of safeguards (or even the perception of a lack of implemented safeguards) can impact trust and reputation. 8,12 - New technologies and cloud applications may facilitate data-in-use protections for researchers and their partners. |
| Protect | Data Security | **PF** | **PR.DS-P5:** Protections against data leaks are implemented. | 2 | **1** | 2 | 2 | **1** | 2,3,4,5,7 - Organizations identify where privacy risk to donors and relatives might arise from data leaks and implement protections commensurate with their risk strategy to comply with consent requirements.  8 - Researchers ensure that all partners implement appropriate protections from device to data storage. Too often, sunset datasets are left unprotected and sunset equipment is disposed of without removing stored data.  12 - Organizations ensure that new technologies provide adequate protections against data leaks. |
| Protect | Data Security | **CSF** | **PR.DS-11:** Backups of data are created, protected, maintained, and tested | **1** | 2 | 2 | 2 | 2 | 1,10 - Backups enable recovery from an incident involving data quality issues or loss of sensitive data, including IP. This practice helps ensure provenance and manage data quality by providing a trusted state to restore to.  2,4,5 - Backups provide benefits but may also be an attack vector for sensitive privacy data. Backups will therefore include appropriate protections.  8 - Ransomware has become a primary threat for researchers. Genomic data continues to be a valuable target. Backups are the primary tool supporting data recovery. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P3:** Backups of information are conducted, maintained, and tested. | 2 | 3 | 2 | 3 | 3 | 1,8,10 - Backups directly impact the ability to have trusted data quality and provenance when there are issues involving the production data. Due to the value of genomic data, including IP, backups may serve to protect the investment in datasets despite the cost of storing such large datasets. Backups can reduce the time it takes to resume operations after an incident. 12 - Whenever new technologies are introduced, the risk becomes higher for data issues, and backups may be considered a higher priority. |
| Protect | Platform Security | **CSF** | **PR.PS-01:** Configuration management practices are established and applied | **1** | 2 | 2 | 2 | 2 | 1,3,6,10 - Configuration management practices reduce the attack surface by minimizing vulnerabilities that may result in issues with data quality, provenance, data access, susceptibility to removable media attacks, and exposed IP.  2,4,5 - Configuration management processes ensure that systems and environments maintain privacy-related cybersecurity capabilities as changes occur over time and that privacy protections (e.g., minimization, consent) remain in place throughout such changes.  8,12 - Data-sharing environments implement effective configuration management control to protect data, analyses, and results, managing risks for sensitive information (e.g., stolen data or misuse) by ensuring authorized access to research results. Technology solutions will include recommended secure configurations. |
| Protect | Protective Technology | **PF** | **PR.PT-P1:** Removable media is protected and its use restricted according to policy. | 2 | 3 | 3 | 3 | 3 | 1,4,7 - When removable media is used, policies will help protect the media and the data’s provenance, preventing data leaks and unauthorized use. 8 - Use of removable media introduces risks in protecting data when sharing among research partners. Enhanced or additional protections may be required as more researchers and partners gain access to genomic data. Organizations may need to limit use of removable media due to increased risk of loss and theft and because of other information beyond the genome. |
| Protect | Protective Technology | **PF** | **PR.PT-P2:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | **1** | 3 | 2 | **1** | 2 | 4,5 - Least functionality helps reduce risks to data exposure and associated privacy risks. 6,12 - Least functionality ensures access is limited to the minimum necessary and restricted to only the data required, particularly when sharing or coordinating across multiple organizations. Least functionality helps achieve minimally necessary access and for only that data someone should be granted access to, especially in sharing or coordination with multiple organizations. Least functionality will have the highest degree of protection and will be enforced on all new technologies. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality). | **1** | 2 | 2 | 2 | 2 | 1 - Baselines ensure an understanding of the expected environment when monitoring for changes or issues with data processing and quality. 3,4 - Configurations will be used to optimize protective technologies to reduce privacy risk and align with consent. 12 - New technologies will incorporate configuration management baselines to ensure least functionality and ensure the platform, device, or software doesn’t introduce additional privacy or security risks. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P2:** Configuration change control processes are established and in place. | **1** | 3 | 2 | 3 | 2 | 1,3,6 - Change control reduces the risk of unauthorized changes that may impact data access, quality, or provenance and ensures that risks from new changes are evaluated. 2,4,5 - Change control will monitor for changes that may impact the effectiveness of privacy controls and the ability to manage consent.  12 - Change control for new technologies will be used to ensure unauthorized changes don’t occur that introduce additional privacy or security risks. |
| Protect | Platform Security | **CSF** | **PR.PS-02:** Software is maintained, replaced, and removed commensurate with risk | 2 | 2 | 2 | 2 | 2 | 1,3,6,7 - Proper software maintenance throughout its life cycle mitigates vulnerabilities and helps maintain data quality and provenance. Effective software management includes processes for approving the use of open-source software, monitoring remote access, implementing patches, and vulnerability management.  2,4,5 - Some software vulnerabilities may introduce privacy risks that lead to problems for individuals (e.g., discrimination, loss of autonomy, loss of trust) and related risks for the organizations (e.g., compliance, reputation).  9 - Laws or guidance may stipulate migration away from unsupported software. Federal organizations follow legal and regulatory requirements for vulnerability management programs, including time to mitigate high or critical vulnerabilities [18]. |
| Protect | Data Security | **PF** | **PR.DS-P3:** Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition. | **1** | 2 | 2 | 3 | **1** | 1,10,12 - This helps establish and trace data and IP ownership and provenance to manage data throughout its life cycle. 8 - Security to protect against data leaks is needed at all steps in research, from device to data storage. Too often, sunset datasets are left unprotected and sunset equipment is disposed of without removing stored data. As more researchers gain access to genomic data, enhanced or additional protections may be required. 9 - Organizations will comply with legal and regulatory requirements for destruction and proper disposal. 12 - Organizations implementing new technologies manage both the disposal of old devices and the acquisition of any new devices to protect the data. |
| Protect | Data Security | **PF** | **PR.DS-P6:** Integrity checking mechanisms are used to verify  software, firmware, and information integrity | 2 | 3 | 2 | 3 | 3 | 1,6,12 - Integrity checking enforces consistent security practices that manage provenance, ensure data quality, and restrict access. These integrity checking mechanisms are necessary for PETs testing and verification and could be helpful for emerging technologies. |
| Protect | Maintenance | **PF** | **PR.MA-P2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access. | 2 | 3 | 3 | 3 | 3 | 1,4,9 - Access (whether authorized or unauthorized) as part of remote maintenance to devices and machines needs to be controlled to prevent people from accessing, modifying, or deleting sensitive information and supports appropriate use of data consistent with consent or legal/regulatory compliance. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P10:** A vulnerability management plan is developed and implemented. | 2 | 3 | **1** | 3 | 3 | 3 - These plans provide the vulnerability inputs to risk modeling and management.  4,5 - Vulnerabilities may directly impact privacy and consent and will be tracked comprehensively to manage associated risks. 12 - The plan will include provisions for how to manage vulnerabilities introduced in new technologies and ensure that contracts with technology providers incorporate sufficient support to ensure remediation of vulnerabilities throughout the technology life cycle. |
| Protect | Platform Security | **CSF** | **PR.PS-03:** Hardware is maintained, replaced, and removed commensurate with risk | 2 | 3 | 3 | 3 | 3 | 1,8,10 - Improper use or disposal of unsupported or outdated hardware introduces risks that may threaten data quality, provenance, and access to sensitive data including IP. 2,4,5 - Managing data on assets, particularly through the disposition process, supports the implementation of privacy requirements, which often include data retention and disposition constraints. 9 - Laws or guidance may stipulate migration away from unsupported hardware. 12 - The hardware used in technology solutions may become outdated and will be replaced following hardware disposal processes to prevent exposing sensitive data. |
| Protect | Data Security | **PF** | **PR.DS-P3:** Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition. | **1** | 2 | 2 | 3 | **1** | 1,10,12 - This helps establish and trace data and IP ownership and provenance to manage data throughout its life cycle. 8 - Security to protect against data leaks is needed at all steps in research, from device to data storage. Too often, sunset datasets are left unprotected and sunset equipment is disposed of without removing stored data. As more researchers gain access to genomic data, enhanced or additional protections may be required. 9 - Organizations will comply with legal and regulatory requirements for destruction and proper disposal. 12 - Organizations implementing new technologies manage both the disposal of old devices and the acquisition of any new devices to protect the data. |
| Protect | Data Security | **PF** | **PR.DS-P8:** Integrity checking mechanisms are used to verify  hardware integrity | 2 | 3 | 2 | 3 | 3 | 1 - Integrity checking for hardware may be prioritized to manage data quality and chain of provenance. 12 - Emerging technologies may use integrity checking mechanisms and ensure that hardware devices are from approved sources, noting that laws may ban the use of hardware from certain nation states. |
| Protect | Maintenance | **PF** | **PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. | 2 | 3 | 3 | 3 | 3 | 1,4,5,6,10 - Logging maintenance and repairs impacts an organization’s ability to manage data, protect IP, and maintain quality, using audits of such activities to establish and trace data ownership and provenance. Logging also supports tracking who accessed privacy data to manage consent. |
| Protect | Platform Security | **CSF** | **PR.PS-04:** Log records are generated and made available for continuous monitoring | **1** | 2 | **1** | 2 | 2 | 1,3,6,8,10,12 - Generating log records helps manage data quality, provenance, and data access. Logs facilitate accountability in the event of unauthorized or malicious activity. All devices and software will be monitored and support logging. 2,4,5 - Log records may help detect and understand privacy events related to unauthorized access or disclosure. 6,8,12 - Organizations with remote maintenance of shared and cloud environments will take extra precautions to implement effective access controls, such as generating log records, that support event correlation to detect malicious behavior. 9 - Log records verify compliance, identify noncompliance, and support legal discovery. |
| Control | Data Processing Management | **PF** | **CT.DM-P8:** Audit/log records are determined, documented,  implemented, and reviewed in accordance with policy and incorporating the principle of data minimization | **1** | 2 | 2 | 2 | 2 | 2,4,5,7 - Audit records can help identify data exposure, unauthorized access, or the extent of a data breach to determine who needs to be notified and whether consent was managed appropriately. Logs help monitor data access to prevent hoarding of donor data and making unwanted changes, as well as to manage changes to individuals’ preferences and consent. Data marked for deletion that has not been deleted may be identified. 12 - New technologies support audit logging to be accountable for whatever happens with the data. |
| Protect | Platform Security | **CSF** | **PR.PS-05:** Installation and execution of unauthorized software are prevented | **1** | 3 | 2 | 2 | 2 | 1,3,6,8,10 - Providers, research environments, and those with IP use these capabilities to prevent inadvertently sharing malicious software with partners that may compromise sensitive data. 12 - New technologies support software asset management by identifying all software used by the technology through an SBOM, interoperability with software monitoring, and proper logging of all software activity. |
| Protect | Platform Security | **CSF** | **PR.PS-06:** Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle | **1** | 2 | 2 | 2 | 2 | 1,6, 8,10,12 - Secure software and system development life cycle principles implement and manage controls for systems throughout the genomic data life cycle that reduce the risk of issues with data quality, provenance, access, IP protection, and new technologies. 2,4,5 - The secure software development life cycle includes processes and activities that address the privacy risks associated with processing genomic data (e.g., privacy engineering practices). |
| Control | Data Processing Policies, Processes, and Procedures | **PF** | **CT.PO-P4:** A data life cycle to manage data is aligned and implemented with the system development life cycle to manage systems. | **1** | 2 | 2 | 2 | 2 | 1, 3 - Data and system life cycles integrate risk management processes and protect data quality and provenance. 4,12 - Consent will be managed throughout data and system life cycles, with special care to address data aggregation and possible re-assessment when technologies enable new processing capabilities and privacy engineering practices. 9 - Governance and regulatory compliance may focus on an organization’s ability to manage data and system life cycles. |
| Protect | Technology Infrastructure Resilience | **CSF** | **PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage | 2 | **1** | 2 | 2 | **1** | 2,4,5,10 - These controls help protect sensitive data, including privacy data and IP. 3 - Risk models identify ways to mitigate the risks of using cloud environments or other environments with remote access. Network access and integrity tools help manage these security risks. 8,12 - Organizations operating collaborative data-sharing environments prevent data from being exposed or altered by implementing remote and logical access controls consistently, using network integrity controls, and restricting use of sensitive data in non-production environments. |
| Protect | Protective Technology | **PF** | **PR.PT-P3:** Communications and control networks are protected. | 2 | 3 | 3 | 3 | 3 | 1,12 - May be relevant to data storage and analysis needs within an organization or when using emerging technologies for transferring data. 8 - Protecting research networks may require technical security solutions that can help with wider data sharing with the research community. |
| Protect | Data Security | **PF** | **PR.DS-P7:** The development and testing environment(s) are separate from the production environment. | 2 | 3 | 3 | 3 | 3 | 3 - Risk assessments will identify potential risks for cloud-based processing in development and testing environments, which will generally be protected like a production environment. Highly sensitive data may exist in criminal justice, healthcare, and clinical lab environments. 4 - Organizations will be cautious with risks associated with AI model development and consent. While typically not taking operational action based on processing in development and testing environments, data security best practices will be used to ensure data privacy by protecting against leaks and breaches. Protecting non-production environments reduces the risk of genomic data being used without consent. |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P3:** Remote access is managed | 2 | 3 | 2 | 2 | 2 | 1,9 - Some organizations may decide to manage remote access in a way that will prohibit local downloading of data (e.g., biobanks, commercial terms) to comply with legal /regulatory requirements around downloading. 2,4,5 - Remote access across partners will implement consistent, appropriate privacy protections according to consent requirements. 6,8 - All forms of remote access, including vendor updates and maintenance and access to research environments, will be managed. 12 - Technologies bring people to data via remote access. Authorized individuals need access to effective, controlled data sharing capabilities. Adopting zero trust principles remains relevant in this case, especially with the increased practice of using remote access [e.g., 21st Century Cures Act allows remote access to personally identifiable information (PII) in research [20].] |
| Protect | Identity Management, Authentication, and Access Control | **PF** | **PR.AC-P5:** Network integrity is protected (e.g., network segregation, network segmentation). | 2 | 3 | 3 | 3 | 3 | 1 - Segmentation supports minimizing uncontrolled or unauthorized access that impacts data quality. 3,12 - Segmentation is a component of remote access and zero trust. 6 - Segmentation prevents unauthorized access and manages authorized access. Control of network segments supports access controls to help prevent privilege escalation. 10 - Organizations may keep information regarding IP in a separate network segment. |
| Protect | Technology Infrastructure Resilience | **CSF** | **PR.IR-02:** The organization's technology assets are protected from environmental threats | 2 | 2 | 2 | 2 | 2 | 3 - Organizations consider known environmental threats (e.g., wildfire, flooding, excessive heat or humidity) where organizational equipment may be located or housed. 8,10,11,12 - Shared data processing environments will incorporate protections for locally stored data and meet legal requirements (e.g., Clinical Laboratory Improvement Amendments). |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P4:** Policy and regulations regarding the physical operating environment for organizational assets are met. | 3 | 3 | 3 | 2 | 3 | 3,8,12 - Organizations will want to manage risks to sequencers and other equipment, including new technologies. |
| Protect | Technology Infrastructure Resilience | **CSF** | **PR.IR-03:** Mechanisms are implemented to achieve resilience requirements in normal and adverse situations | 3 | 3 | 3 | 3 | 3 | 1,3,8 - Availability, as ensured by resilience mechanisms, is important for MOs where information or research is being shared across a supply chain.  9 - Certain sectors may have laws or regulations that stipulate uptime requirements that would require resilience mechanisms. 10 - Organizations protecting IP may prioritize resilience higher, potentially in cases where the use of the IP is tied to outcomes that may be potentially impacted by outages. 12 - New technologies will be selected to meet organizational resilience requirements. |
| Protect | Protective Technology | **PF** | **PR.PT-P4:** Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations. | 3 | 3 | 3 | 3 | 3 | 8,12 - Resiliency mechanisms may be prioritized in certain environments (e.g., hospitals) and can help with the availability of data sharing with the research community. |
| Protect | Technology Infrastructure Resilience | **CSF** | **PR.IR-04:** Adequate resource capacity to ensure availability is maintained | 3 | 3 | 3 | 3 | 3 | 8,10 - Capacity and availability will be a higher priority in data-sharing environments, particularly if they are for time-sensitive applications such as healthcare. |
| Protect | Data Security | **PF** | **PR.DS-P4:** Adequate capacity to ensure availability is maintained. | 2 | 3 | 3 | 3 | 3 | 2,5 - Capacity can directly impact individuals when decisions are being made about them based on their data.  6 - Adequate availability reduces the need to download genomic data. 12 - Organizations will ensure that new technologies support data availability requirements. |
| Detect | Continuous Monitoring | **CSF** | **DE.CM-01:** Networks and network services are monitored to find potentially adverse events | 2 | 3 | 3 | 3 | 3 | 1 - Organizations monitor for data quality and provenance issues throughout the life cycle. 2,4,5 - Monitoring will detect when privacy data has been accessed inappropriately. 6,8,10,12 - Network monitoring helps protect data (e.g., IP, new technology) and sensitive research from events such as unauthorized access or ransomware. 9 - Monitoring supports legal discovery. |
| Detect | Continuous Monitoring | **CSF** | **DE.CM-02:** The physical environment is monitored to find potentially adverse events | 3 | 3 | 3 | 3 | 3 | 6 - Organizations monitor the physical environment for unauthorized access, including to physical assets or genomic data processing components. Threat modeling has demonstrated that physical environments can be a significant area of risk.  10 - Monitoring physical access to any facilities where IP is stored supports incident investigations. |
| Detect | Continuous Monitoring | **CSF** | **DE.CM-03:** Personnel activity and technology usage are monitored to find potentially adverse events | **1** | 3 | 2 | 2 | 2 | 1,2,4,5,6,10 - Personnel access to sensitive data (e.g., privacy data, IP) will be restricted and monitored to detect activity (e.g., unauthorized access) that could compromise data and its integrity or provenance. 8,12 - Managing personnel activity will be prioritized in environments that share space and physical access, such as research or academic environments. |
| Detect | Continuous Monitoring | **CSF** | **DE.CM-06:** External service provider activities and services are monitored to find potentially adverse events | **1** | 3 | 2 | 2 | 2 | 1,6,8 - All parties in data-sharing environments will have detection processes in place to consistently protect data quality throughout the life cycle. Monitoring will be consistent across external service providers through the implementation of the same or comparable access controls and the willingness to share monitoring alerts.  10 - Sensitive data may be targeted by external providers; organizations detect unauthorized attempts to access sensitive data such as IP. 12 - Organizations monitor new technologies to ensure they are functioning as designed. |
| Detect | Continuous Monitoring | **CSF** | **DE.CM-09:** Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events | 2 | 2 | 2 | 2 | 2 | 2,4,5 - Privacy-related attacks can occur due to integrity issues (e.g., data leaks, malicious code, unauthorized code) with hardware and software. 6,8,10,12 - This monitoring identifies events that may indicate unauthorized access or malicious software that affects the quality of research, IP, or other results.  12 - New technologies may introduce hardware, software, or other data that may disrupt other assets and impact outcomes. |
| Protect | Data Security | **PF** | **PR.DS-P6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity. | 2 | 3 | 2 | 3 | 3 | 1,6,12 - Integrity checking enforces consistent security practices that manage provenance, ensure data quality, and restrict access. These integrity checking mechanisms are necessary for PETs testing and verification and could be helpful for emerging technologies. |
| Protect | Data Security | **PF** | **PR.DS-P8:** Integrity checking mechanisms are used to verify  hardware integrity | 2 | 3 | 2 | 3 | 3 | 1 - Integrity checking for hardware may be prioritized to manage data quality and chain of provenance. 12 - Emerging technologies may use integrity checking mechanisms and ensure that hardware devices are from approved sources, noting that laws may ban the use of hardware from certain nation states. |
| Detect | Adverse Event Analysis | **CSF** | **DE.AE-02:** Potentially adverse events are analyzed to better understand associated activities | **1** | 3 | 2 | 3 | 2 | 1 - Analysis will determine if the attack impacted data quality or provenance. 2,4,5 - Analysis will determine if the attack involves privacy or consent issues. 6,10 - The analysis may determine if the attack exposes sensitive data including unauthorized access or threats to IP. |
| Detect | Adverse Event Analysis | **CSF** | **DE.AE-03:** Information is correlated from multiple sources | 2 | 3 | 3 | 3 | 3 | 1,3,6,8,10 - Correlation facilitates the ability to hunt for similar attacks across the network that may impact data quality, provenance, access, IP, research results, or the data life cycle. 2,4,5 - Correlation can help to coordinate the response to attacks that result in privacy impacts. |
| Detect | Adverse Event Analysis | **CSF** | **DE.AE-04:** The estimated impact and scope of adverse events are understood | **1** | 3 | 2 | 2 | 2 | 1,6,8,10 - Analysis teams will want to understand the nuances of genomic data processing to determine the impact and appropriate response to issues with data quality, provenance, access, research, and IP. |
| Detect | Adverse Event Analysis | **CSF** | **DE.AE-06:** Information on adverse events is provided to authorized staff and tools | 2 | 3 | 2 | 2 | 2 | 2,4,5,6,10 - Organizations processing sensitive data, such as data that impacts privacy and IP, will prioritize detection communication processes higher and ensure that authorized staff are appropriately identified in response plans. |
| Detect | Adverse Event Analysis | **CSF** | **DE.AE-07:** Cyber threat intelligence and other contextual information are integrated into the analysis | 2 | 3 | 2 | 3 | 3 | 1,3,6,8,10 - CTI and related context improve the ability to identify similar attacks across the network that may impact data quality or provenance, or be targeted at research organizations or specific IP. 2,4,5 - CTI and related context may indicate that specific adversaries are using specific TTPs targeted at human genomic data. |
| Detect | Adverse Event Analysis | **CSF** | **DE.AE-08:** Incidents are declared when adverse events meet the defined incident criteria | 2 | 3 | 2 | 2 | 2 | 2,4,5 - Incident criteria include indicators for identifying incidents that have or may impact privacy and that require coordination with the privacy incident response team to determine whether additional privacy response activities are necessary. 6,8,10 - An incident involving data access, research data, or IP will have specific response requirements that include notification of specific teams and response activities. 7 - Thresholds may indicate the need to involve public relations teams if there is a risk to reputation. |
| Respond | Incident Management | **CSF** | **RS.MA-01:** The incident response plan is executed in coordination with relevant third parties once an incident is declared | **1** | **1** | **1** | 2 | **1** | 1,6,8,12 - Response operations manage any impact on data quality and provenance, quickly mitigate any unauthorized access, coordinate across all partners, and address any issues with new technologies. 2,4,5,9 - Organizations execute the incident response plan to manage the impact of privacy breaches in compliance with laws and regulations, communicating the impact on donors and relatives as required. 3 - Executing the response plan puts into practice the risk management activities identified through risk modeling. |
| Respond | Incident Management | **CSF** | **RS.MA-02:** Incident reports are triaged and validated | **1** | **1** | 2 | 2 | **1** | 1,6 - Appropriate response helps manage the impact on data quality, provenance, or access. 2,4,5 - Triage processes help organizations determine the extent of a compromise and whether it affects a donor, donor's relatives, or both, informing genomic data breach responses. 10 - Organizations with IP will want to quickly diagnose any impact on the IP and manage the response appropriately. |
| Respond | Incident Management | **CSF** | **RS.MA-03:** Incidents are categorized and prioritized | **1** | **1** | 2 | 2 | **1** | 1,6,8 - Incidents that impact data quality, provenance, or access are categorized and prioritized to expedite remediation and restore confidence in the data for research or other purposes. 2,4,5,10 - Categorizing ensures that IP and privacy-related incidents are handled with appropriate urgency. |
| Respond | Incident Management | **CSF** | **RS.MA-04:** Incidents are escalated or elevated as needed | 2 | 2 | 3 | 2 | 2 | 1,6,8 - Incidents that impact data quality, provenance, or access (whether unauthorized access by authorized users or access by unauthorized users) are escalated to apply appropriate resources to the incident response and recovery.  2,4,5,10 - Escalation ensures that IP or privacy-related incidents are handled with appropriate urgency. |
| Respond | Incident Management | **CSF** | **RS.MA-05:** The criteria for initiating incident recovery are applied | **1** | 2 | 2 | 2 | 2 | 1,6,10 - Incidents that impact data quality, provenance, access, or IP are evaluated against pre-defined criteria to apply appropriate resources to the incident recovery and coordinate across all partners. 2,4,5 - Applying pre-defined criteria supports an organization's ability to determine if recovery operations (e.g., escalations, notifications) need to be initiated in response to a privacy or consent-related incident. |
| Respond | Incident Analysis | **CSF** | **RS.AN-03:** Analysis is performed to establish what has taken place during an incident and the root cause of the incident | 2 | 2 | 2 | 2 | 2 | 1,6,10 - This analysis helps prevent further incidents, addressing the impact on data quality, provenance, IP, and access. 2,4,5 - Performing analysis, including forensics if needed, determines whether consent agreements were violated and the resulting impact on donors or their relatives. 9 - Establishing what has taken place and the root cause may help identify any legal or regulatory reporting requirements.AE248 |
| Respond | Incident Analysis | **CSF** | **RS.AN-06:** Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved | 2 | 2 | 2 | 2 | 2 | 1,6 - Records can be used to enforce accountability of actions (e.g., access) during an incident and promote transparency of the investigative actions to support the preservation of quality and trustworthy genomic data throughout its life cycle. 3 - Documenting all investigative actions helps identify, model, and mitigate cybersecurity and privacy risks in the processing of genomic data. |
| Respond | Incident Analysis | **CSF** | **RS.AN-07:** Incident data and metadata are collected, and their integrity and provenance are preserved | 3 | 2 | 3 | 3 | 2 | 1 - Proper handling of incident data helps document any issues with data quality and provenance. 2,4,5,6 - Incident data and metadata support investigations that inform privacy impact and an incident's magnitude, allowing for a thorough understanding of how incidents occurred. The data helps document access to sensitive data and ensures that access is managed to prevent corruption or deletion and minimize the likelihood of future incidents. 7,9 - Records may be needed for legal purposes and can be used to demonstrate the vigilance needed to repair reputational issues. |
| Protect | Data Security | **PF** | **PR.DS-P6:** Integrity checking mechanisms are used to verify  software, firmware, and information integrity. | 2 | 3 | 2 | 3 | 3 | 1,6,12 - Integrity checking enforces consistent security practices that manage provenance, ensure data quality, and restrict access. These integrity checking mechanisms are necessary for PETs testing and verification and could be helpful for emerging technologies. |
| Respond | Incident Analysis | **CSF** | **RS.AN-08:** An incident's magnitude is estimated and validated | **1** | **1** | 2 | 2 | **1** | 1,6,10,11 - This assessment helps quantify the full impact on data quality, provenance, IP, and access and may help assess any impact on sample diversity. 2,4,5 - When privacy data is involved, the magnitude of the incident helps determine the specific reporting requirements and activities needed to prevent further issues. |
| Respond | Incident Response Reporting and Communication | **CSF** | **RS.CO-02:** Internal and external stakeholders are notified of incidents | 2 | 2 | 2 | **1** | 2 | 1,8 - Any impact on data quality or provenance is communicated to stakeholders and partners who share the data or results from processing the genomic data.  2,4,5 - Consent is managed across the data life cycle, and issues with consent require taking action, including notification. A privacy breach requires the organization to notify donors and inform them of any issues with consent. Public notification of the breach may be the only way to help relatives identify that there may be an issue with their data. 9 - Notification is required legally for certain types of incidents, such as privacy breaches. 11 - Communicating incidents that affect sample diversity helps affected populations understand any potential impact on sample diversity. |
| Respond | Incident Response Reporting and Communication | **CSF** | **RS.CO-03:** Information is shared with designated internal and external stakeholders | 2 | 2 | 2 | 2 | 2 | 1,8 - Communication promotes repairing any issues with trusting data provenance and integrity as needed for research partners. 2,4,5 - Coordination with designated stakeholders helps manage privacy response and recovery activities. 6 - Communicating how TTPs resulted in unauthorized access can help stakeholders improve their defenses against similar attacks. |
| Respond | Incident Mitigation | **CSF** | **RS.MI-01:** Incidents are contained | **1** | **1** | 2 | 2 | **1** | 1,6 - Containment prevents further impact on data quality and provenance while minimizing unauthorized access to data. 2,4,5 - Containment limits the impact of privacy-related incidents. 8,10,12 - Containment helps limit the impact on IP across research partners and from technology solutions. |
| Respond | Incident Mitigation | **CSF** | **RS.MI-02:** Incidents are eradicated | **1** | **1** | 2 | 2 | **1** | 1,6 - Eradication prevents further impact on data quality and provenance and minimizes the potential for additional unauthorized access to data. 2,4,5 - Eradication helps prevent further impact of privacy-related incidents. 8,12 - Eradication helps stop the impact on IP across research partners and from technology solutions. |
| Recover | Incident Recovery Plan Execution | **CSF** | **RC.RP-01:** The recovery portion of the incident response plan is executed once initiated from the incident response process | **1** | 2 | 2 | 2 | 2 | 1,8,11,12 - Recovery plan activities coordinate across partners to track progress toward being able to trust the data and return to normal operations. Involving all partners and technology solutions helps ensure comprehensive recovery.  2,4,5,9 - Recovery activities address legal, policy, regulatory, privacy, and consent requirements. 3,10 - The recovery plan manages high-risk recovery operations and impacts to IP. Risk modeling and tolerances may help determine the scope and resourcing required to manage recovery operations. 6 - Recovery plans incorporate and enforce data access protection requirements, including access control for backups. 7 - Recovery plans include communications required to maintain and restore trust in the organization. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P7:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | 2 | 3 | 2 | 3 | 2 | 2,4,5,9 - Response plans will include appropriate actions to identify, manage, and recover from privacy breaches, including notifying donors, returning to an acceptable state in accordance with consent agreements, and complying with legal and contractual requirements. 3 - Risk management strategies will include appropriate response planning and processes including managing any adverse outcomes to individuals affected. 7 - Response and recovery activities will directly impact an organization’s reputation and the trust of partners who rely on the organization.  10 - Response and recovery plans identify any IP and associated activities to protect it and recover so that IP data is available to be used for business purposes. |
| Recover | Incident Recovery Plan Execution | **CSF** | **RC.RP-02:** Recovery actions are selected, scoped, prioritized, and performed | **1** | 2 | 2 | 2 | 2 | 1,10 - Prioritized recovery actions include those that restore data quality, protect provenance, and protect IP.  2,4,5,9 - Prioritize recovery actions that address legal, policy, regulatory, privacy, and consent requirements.  7 - Prioritized recovery actions include those that maintain and restore the trust in and reputation of the organization. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P8:** Response and recovery plans are tested. | 2 | 2 | 2 | 3 | 2 | 2,5 - Testing plans ensures that response and recovery activities are effective to limit the privacy impact of an incident and recover to an acceptable state. 8,12 - When new technologies are introduced, there may be special needs for response and recovery to ensure that teams understand any new requirements. Additionally, testing helps ensure that response and recovery across partners are effective. |
| Recover | Incident Recovery Plan Execution | **CSF** | **RC.RP-03:** The integrity of backups and other restoration assets is verified before using them for restoration | **1** | 2 | 2 | 2 | 2 | 1,10 - Backups enable recovery from an incident involving data quality issues or loss of sensitive data, including IP. Verifying integrity identifies any data tampering that may impact data quality, provenance, or compromise.  2,4,5 - Backups provide benefits but may also be an attack vector for privacy data. Enterprise and system management plans consider both the roles and risks of backup management, including checks to verify privacy data quality. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P3:** Backups of information are conducted, maintained, and tested. | 2 | 3 | 2 | 3 | 3 | 1,8,10 - Backups directly impact the ability to have trusted data quality and provenance when there are issues involving the production data. Due to the value of genomic data including IP, backups may serve to protect the investment in datasets despite the cost of storing such large datasets. Backups can reduce the time to resume operations after an incident. 12 - Whenever new technologies are introduced, the risk becomes higher for data issues, and backups may be considered higher priority. |
| Recover | Incident Recovery Plan Execution | **CSF** | **RC.RP-04:** Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms | 2 | 3 | 2 | 2 | 3 | 8 - Research-heavy organizations will want to know when restoration of systems has occurred and whether the data used in research is available and of trustworthy quality. 12 - When new technologies are impacted by an incident, post-incident activities ensure that any vulnerabilities have been addressed and that new post-operational norms include implementing additional or new cybersecurity risk management activities moving forward. |
| Identify | Business Environment | **PF** | **ID.BE-P2:** Priorities for organizational mission, objectives, and activities are established and communicated. | 3 | 3 | 2 | 3 | 3 | 9 - Prioritize legal compliance to ensure business viability.  10 - Organizations with IP prioritize protecting inventions and investments. 11 - Diversity needs vary based on the context of processing and may require coordination with multiple organizations. Clearly communicate priorities related to diversity to influence operations. 12 - Priorities determine how forward-leaning the organization is when embracing privacy-enhancing and secure technologies; ID.BE-P1 and -P3 more directly influence technology decisions. |
| Recover | Incident Recovery Plan Execution | **CSF** | **RC.RP-05:** The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed | **1** | 2 | 2 | 2 | 2 | 8 - Researchers will want to verify that both they and their suppliers and partners have fully checked asset integrity to confirm recovery status. 12 - When new technologies are impacted by an incident, Recover activities ensure that any asset integrity issues have been addressed. |
| Protect | Data Security | **PF** | **PR.DS-P8:** Integrity checking mechanisms are used to verify  hardware integrity. | 2 | 3 | 2 | 3 | 3 | 1 - Integrity checking for hardware may be prioritized to manage data quality and chain of provenance. 12 - Emerging technologies may use integrity checking mechanisms and ensure that hardware devices are from approved sources, noting that laws may ban the use of hardware from certain nation states. |
| Recover | Incident Recovery Plan Execution | **CSF** | **RC.RP-06: T**he end of incident recovery is declared based on criteria, and incident-related documentation is completed | 2 | 3 | 3 | 3 | 3 | 1,3,6,10,12 - Documenting and resolving incident-related lessons learned will help reduce the likelihood of future incidents.  2,5 - Post-incident recovery activities will include confirmation that any incidents involving privacy-related breaches have been addressed. |
| Protect | Data Protection Policies, Processes, and Procedures | **PF** | **PR.PO-P7:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed. | 2 | 3 | 2 | 3 | 2 | 2,4,5,9 - Response plans will include appropriate actions to identify, manage, and recover from privacy breaches, including notifying donors, returning to an acceptable state in accordance with consent agreements, and complying with legal and contractual requirements. 3 - Risk management strategies will include appropriate response planning and processes including managing any adverse outcomes to individuals affected. 7 - Response and recovery activities will directly impact an organization’s reputation and the trust of partners who rely on the organization.  10 - Response and recovery plans identify any IP and associated activities to protect it and recover so that IP data is available to be used for business purposes. |
| Recover | Incident Recovery Communication | **CSF** | **RC.CO-03:** Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders | **1** | **1** | 2 | **1** | **1** | 1 - Communication throughout the genomic data life cycle helps organizations maintain trust in data quality and improve future outcomes.  2,4,5,9 - Applicable laws and regulations often include communication requirements regarding privacy and consent, such as breach notification. While it may be particularly difficult to contact relatives, organizations will determine what processes need to be developed to communicate with or contact relatives of donors. 7,8 - Recovery communications help organizations, including researchers, repair their reputations and maintain access to trusted data sources. |
| Recover | Incident Recovery Communication | **CSF** | **RC.CO-04:** Public updates on incident recovery are shared using approved methods and messaging | 2 | 2 | 2 | 2 | 2 | 2,7 - Public relations may be the primary way that relatives interact with genomic data. Poor public relations and lack of public updates can impact reputation and whether individuals will trust the organization in the future. Good public relations with timely and clear updates can rebuild and extend trust. 4,5 - Public perception could limit future donors if they do not trust the organization to manage privacy or consent. 8,10,12 - Public perception of researchers, businesses with genomic IP, and new genomic technologies could impact the use and adoption of the organization’s output. Managing public perception promotes trust. |