Extracted Questions and Answers from NIH Security Best Practices for Users of Genomic Controlled Access Data Day 1

Question	Answer
How much amount of time to remediate?	Time to remediate and milestone items are specific to the organization but should be aligned to best efforts to resolve in a timely manner without unreasonable delay and based on the risk of potential impact.
Do Docker images need to have baseline configuration and vulnerability scans before they're allowed to handle NIH controlled access data?	Yes, vulnerability monitoring and scanning is part of the NIST 800-171 control families. The expectation is that systems undergo vulnerability monitoring and scanning as appropriate for processing NIH controlled access data. The types of scans and frequency are organizationally defined.
Does NIH intend for security controls to apply to data created through the processing or analysis of controlled access genomic data? If so, what derived data would be considered restricted and what data are subject to these controls?	NIH expects users and their institutions to protect data obtained from the listed controlled access repositories according to NIST 800-171. All types of derived data are protected, for instance, derived data such as SNPs are also expected to be secured similarly to individual controlled access data.
What examples are there of developers at universities that are also not researchers?	The focus is on those that are funded by NIH to do the work. Developers establish, support, or maintain an NIH-controlled repository. If a PI is funded to develop tools for a specific repository, they are considered a developer. If they are developing a tool for general use, that would be classified as research.
Is NIH requiring compliance with NIST 800-171 Rev 2 or Rev 3?	NIH will accept both Rev 2 and Rev 3 as fulfilling security expectations. Institutions on Rev 2 should start planning for Rev 3 adoption.
Where can we find the list of subject repositories?	The list of NIH-controlled access repositories is available: https://sharing.nih.gov/accessing-data/NIH-security-best-practices

Does NIH consider controlled access genomic data to be CUI?	No, NIH does not consider this data to be CUI but is using the NIST 800-171 security controls as a best practice for data protection.
What is the definition of a developer?	This is based on an awardee funded to do particular work in one of the 20 NIH-controlled repositories.
What are the expectations for data generators such as core facilities, which may end up contributing to one of the databases, like the dbGaP?	The security standards outlined in the update are only aligned to the users of controlled access data from NIH-controlled repositories, not data generators.
How is NIH tracking access to correlate and validate the right people with the right access?	NIH does not apply any identifier to track users when they get access to data or if they're working inside a cloud environment at NIH. What is recorded is the PI's name, institution, and research use statement. When a PI moves institutions, they must close out their project at the old institution and submit a new data access request at the new institution.
Will NIH require an authorized official to submit the attestation, or can researchers submit it directly?	The attestation will be part of the Data Access Request (DAR) process, with the PI and institutional signing official confirming adherence to security best practices.
For long-term attestation, will an individual or an enterprise complete the attestation?	The individual (PI) will attest to protecting the data according to the required security benchmark.
Will the attestation process extend to other repositories or data types?	If a repository includes genomic data and other associated data types, the attestation and security requirements will apply to all data in the repository.
What are the expectations for Plan of Action and Milestones (POAM)?	POAMs should be managed within the institution, documenting planned security improvements. The government does not require submission, but institutions must work toward compliance without unreasonable delay.
Did NIH review the financial impact of these new security standards?	NIH considered both the impact on institutions and existing regulations when determining security requirements. The self-assessment and POAM pathway provide flexibility for institutions to work toward compliance without unreasonable delay.
If a researcher submits an attestation without confirming with their	There would be consequences that NIH may follow up as a cybersecurity or data management incident and work with the institution to remediate any plan to be able to meet

institution, could there be consequences?	these security expectations. The institution and researcher could face compliance actions if misleading statements were made.
Why was NIST 800-171 chosen as the standard?	NIST 800-171 aligns with widely used security controls across government agencies, including HIPAA and NIST 800-53. NIH previously had security standards for controlled access data, and this update continues that practice.
If an institution is not fully compliant but has a POAM in place, is that sufficient as of January 25, 2025?	Yes, an institution with a POAM in place can still attest to protecting NIH-controlled access data while working toward full compliance.

Extracted Questions and Answers from NIH Security Best Practices for Users of Genomic Controlled Access Data Day 2

Question	Answer
Are workstations that interact with the system in scope?	Yes, workstations that interact with NIH-controlled access data are within scope. Any system that downloads, processes, accesses, transmits, or stores NIH-controlled access data applicable to the NIH Genomic Data Sharing Policy is within scope.
If you have genomic data from one base needed for performance of an NIH-funded grant, will the cost of compliance be chargeable as a direct cost to the grant?	The answer depends on NIH's Grants Management Team. The specifics of the award and how the data is managed and shared will determine if compliance costs can be charged as direct costs. Contact NIH's Grants Management Team for more insight.
What are researchers certifying to? Will only researchers that need to meet NIST 800-171 be asked to certify?	Researchers will attest that their institution has performed a self-assessment of their system's compliance with NIST 800-171 security controls, and either the controls are in place or there is a plan of action in place. The attestation applies only to systems storing controlled-access human genomic data, not to the entire institution. The attestation is signed by the Principal Investigator (PI) and the Institutional Signing Official.

Given the short notification time, is NIH considering extending the deadline for implementation?	No, NIH is not considering extending the deadline. The guide notice was released in July 2024, allowing institutions sufficient time to self-assess and develop plans of action and milestones for compliance. Attestations are to be established by the deadline.
Is data processed on the NIH server covered?	The requirement applies when a PI submits a Data Access Request to one of the 20 listed repositories. When downloaded, that data is expected to be secured according to NIST 800-171. If using an NIH-provided secure processing environment like the TopMed Imputation Server, those environments already meet the necessary security standards. The security standard applies primarily to downloaded and stored data.
What is the minimum encryption strength to store NIH-controlled genomic data?	Encryption must be compliant with FIPS 140-3 standards. While AES-128 is FIPS-approved, users should verify their encryption protocols align with the latest compliance requirements listed in NIST 800-171 references.
In the event of an unapproved access incident, what actions could NIH take?	The Data Use Agreement specifies how to handle cybersecurity or data management incidents. NIH expects timely reporting and cooperation from the approved user to resolve and mitigate future risks. Specific compliance actions would depend on the nature of the incident.
Do the NIST 800-171 requirements apply to any data downloaded from a controlled-access repository or only to genomic data?	The requirement applies to all data obtained from an NIH-controlled access repository, not just genomic data. If genomic and associated data are retrieved, they must be secured per NIST 800-171.
Will the Signing Official attestation always be required, or will some repositories rely exclusively on PI attestation?	Both the PI and the Institutional Signing Official must attest. This maintains consistency with existing Data Access Request processes.
Are there future plans to require NIST 800-171 environments to be CMM Level 2 certified?	No, NIH does not plan to require CMM Level 2 certification. NIST 800-171 was selected as the security standard because it aligns with other federal agencies' requirements and provides consistency for NIH funding applicants.
Will an ISO 27001 certification be accepted as attestation?	Yes, ISO 27001/27002 is a generally accepted equivalent for international users who cannot attest to NIST 800-171. NIH is also open to reviewing other international cybersecurity standards.

How does controlled-access genomic data relate to Controlled Unclassified Information (CUI)?	NIH does not classify controlled-access genomic data as CUI. The focus of the update is to align with NIST 800-171 security controls rather than to designate data under CUI.
Where will investigators see the attestation requirement?	For repositories like dbGaP, the attestation will appear in the Data Access Request process as a required check box before submission.