



## Acceptable Use Policy

---



Bionimbus Protected Data Cloud

Version 1.1

2016

## **THE PROTECTED DATA CLOUD (PDC) ACCEPTABLE USE POLICY FOR INFORMATION TECHNOLOGY**

The purpose of the policy is to establish and promote the ethical, legal and secure use of computing and electronic communications for all members of the community. The policy applies to everyone who uses PDC information technology resources and to all uses of those resources, whether physically located on campus or remotely.

The environment of free expression and the diversity of perspectives inherent in an academic institution are essential to our values and the nature of PDC. At the same time PDC may be required by law to access and disclose information from computer and network user accounts or may find it necessary to do so in order to protect PDC's legal interests, uphold contractual obligations or comply with other internal or external policies. It may also be required to access information to diagnose and correct technical problems.

PDC reserves the right to access and disclose information as required by law, to uphold contractual obligations, to enforce PDC policies or to diagnose and correct technical problems. Compliance with applicable law and/or PDC's legal interests may require accessing, viewing and/or preserving data relevant to pending or potential litigation. This is true regardless of whether the data is stored on computers owned by PDC, private individuals or other entities.

When any use of information technology at PDC presents an imminent threat to other users or to PDC's technology infrastructure, system operators may, without notice to the user, take whatever steps are necessary to manage the threat. This may include changing passwords, removing access rights, disabling or impounding computers, or disconnecting specific devices or entire network segments from voice and data networks. System operators will restore connectivity and functionality as soon as possible after they identify and neutralize the threat.

Users are responsible for protecting their account credentials and may not share those credentials with any person, including IT support staff.

PDC reserves the right to limit access to its networks or to remove materials stored or posted on its computers when applicable policies, contractual obligations, or applicable laws are violated. In addition, users bear a personal responsibility to comply with all PDC policies, contractual obligations and applicable laws and regulations, including protecting the private information of others. Alleged violations will receive the same due process as any other alleged violation of policy, contractual obligations, or applicable laws.



## Code of Conduct

---



Bionimbus Protected Data Cloud

Version 1.1

2016

## OVERVIEW

Code of Conduct (also referred to as Rules of Behavior) describe security controls associated with user responsibilities and certain expectations of behavior for following security policies, standards, and procedures. Security control PL-4 requires Bionimbus Protected Cloud Service Providers to implement the Code of Conduct.

The Code of Conduct may be signed on paper or electronically at first login. Either way, the organization must retain artifacts to enable an independent assessor to verify that the code of conduct has been signed for all users.

## PDC APPROVED USER CODE OF CONDUCT

The following is the Code of Conduct that research investigators agree to abide by as an Approved User of data received through dbGaP and PDC. Failure to abide by any term within this Code of Conduct may result in revocation of approved access to any or all datasets obtained through PDC.

The elements of the NIH Code of Conduct for Genomic Data Use include:

1. Investigator(s) will use requested datasets solely in connection with the research project described in the approved Data Access Request for each dataset;
2. Investigator(s) will make no attempt to identify or contact individual participants from whom these data were collected without appropriate approvals from the relevant Institutional Review Boards;
3. Investigator(s) will not distribute these data to any entity or individual beyond those specified in the approved Data Access Request;
4. Investigator(s) will adhere to computer security practices that ensure that only authorized individuals can gain access to data files;
5. Investigator(s) acknowledge the Intellectual Property Policies as specified in the Data Use Certification obtained on approval of your Data Access Request; and,
6. Investigator(s) will report any inadvertent data release in accordance with the terms in the Data Use Certification obtained on approval of your Data Access Request, breach of data security, or other data management incidents contrary to the terms of data access.

### ACCEPTANCE AND SIGNATURE

I have read the above *Code of Conduct* for Bionimbus Protected Data Cloud systems and networks. By my electronic acceptance and/or signature below, I acknowledge and agree that my access to all Bionimbus Protected Data Cloud systems and networks is covered by, and subject to, such Rules. Further, I acknowledge and accept that any violation by me of these Rules may subject me to civil and/or criminal actions and that Bionimbus Protected Data Cloud retains the right, at its sole discretion, to terminate, cancel or suspend my access rights to the Bionimbus Protected Data Cloud systems at any time, without notice.

O

---

*Comments here:*



THE UNIVERSITY OF  
**CHICAGO**

# Non Disclosure Agreement

---



OPEN SCIENCE DATA CLOUD



OPEN COMMONS CONSORTIUM

## Bionimbus Protected Data Cloud

Version 1.1

2016

## **Bionimbus Protected Data Cloud Non-Disclosure Agreement**

### **COMMITMENT TO PROTECT NON-PUBLIC INFORMATION**

Access to non-public information may be required, while working under the Bionimbus Protected Data Cloud (the "Disclosing Party") for \_\_\_\_\_ (Individual Name) of \_\_\_\_\_ (Organization Name) located at \_\_\_\_\_ (Organization Address) (the "Recipient" or the "Receiving Party").

Should I have access to non-public information, I agree that I shall not release, publish, or disclose such information to unauthorized persons. I shall protect such information and will employ all reasonable efforts to maintain the confidentiality of such information. These efforts shall be no less than the degree of care employed by PDC to preserve and safeguard sensitive information.

**I agree that I shall immediately notify the PDC IT Operations Center of any suspected or confirmed unauthorized disclosure and/or misuse of sensitive information.**

[Contact: Bionimbus Data Cloud Operations Center: [support@opensciencedatacloud.org](mailto:support@opensciencedatacloud.org)]

I understand that there are laws and regulations (that may apply) which provide for criminal and/or civil penalties for improper disclosure, including but not limited to:

- a) 18 U.S.C. 641 (Public Money, Property or Records)
- b) 18 U.S.C. 1832 (Trade Secrets)
- c) 18 U.S.C. 1905 (Disclosure of Confidential Information)
- d) 5 U.S.C. 552a (Privacy Act)

***I have read and understand the requirements stated above and agree to adhere to them for the duration of time I work with the Bionimbus Protected Data Cloud . I understand that violation of the agreement may subject me to criminal and civil penalties.***