

# **Privacy, Security and Data Transaction Policies**

## **Division of Biostatistics**

## Table of Contents

1. Introduction
2. Definition of protected health information
3. The security of PHI and of transactions that may contain PHI
  - A. The security of electronic datasets containing PHI
  - B. The security of floppy disks and other removable media containing PHI
  - C. The security of paper records containing PHI
  - D. The security of e-mail
  - E. The security of websites
  - F. The security of home computers and laptop computers
  - G. The security of FAXes containing PHI
  - H. The security of passwords
  - I. The security of offices and storage rooms containing PHI
  - J. Structure of and access to Biostatistics computing facilities
  - K. Confidentiality agreements
  - L. Reporting privacy breaches
4. Databases
  - A. Definition of a database
  - B. Determining whether protected information is present
  - C. The registration of databases
  - D. The structure of consulting databases
5. Division responsibilities when collaborators violate security and confidentiality obligations
6. Human subjects approvals and consent forms
  - A. Division responsibilities for confirming that collaborators have obtained human subjects approval
  - B. Division response to the absence of human subjects approval
  - C. Division procedures regarding the time period during which data can be analyzed
  - D. Revocation of permission to use data
  - E. Data use agreements
7. Datasets used for instructional purposes
8. Genetic data
  - A. Genotype data
  - B. Pedigree structure

9. Access by individuals to Protected Health Information
10. Accounting for Disclosures of Protected Health Information
11. Amendment of Protected Health Information
12. Authorization for use or disclosure of Protected Health Information
13. Use or disclosure of Protected Health Information with Business Associates
14. Appropriate methods of communicating Protected Health information
15. Use or disclosure of PHI in fundraising
16. Use or disclosure of PHI in marketing
17. Use or disclosure of PHI in media relations
18. Minimum necessary request, use or disclosure of Protected Health Information
19. Distribution of Notice of Privacy Practices
20. Use or disclosure of Protected Health Information without a verbal or written agreement
21. Use or disclosure of psychotherapy notes

**1. Introduction:** The purposes of this document are to detail the policies and procedures that govern the handling of protected health information (PHI) and human subjects approval within the Division of Biostatistics. Specifically, we discuss Division guidelines as they relate to the security of PHI, our approach to collaborative relationships that may include the analysis or transmission of PHI, our handling of databases containing PHI, and our role in ensuring that proper human subjects approvals have been obtained in all of our research activities. We discuss these issues as they apply both to ad hoc consulting relationships and to collaborative research both within and without Washington University. Our intent is to meet or exceed all mandates put forth by the Health Insurance Portability and Accountability Act (HIPAA) and by relevant Washington University policies regarding the privacy and security of PHI that is under our direct control, of PHI that is transferred by us to collaborators and other individuals, and of the manner in which PHI is transferred by others to us. The security that is applied to existing PHI will be upgraded to meet all standards that are put forth in this document. Thus, all security standards that are described herein apply equally to all PHI under our control.

Sections 2 through 8 below provide details of procedures that govern the research and instructional activities that constitute the overwhelming bulk of the functioning of the Division of Biostatistics. Sections 9-21 respond briefly to our activities as they relate to specific issues that are itemized in the Washington University HIPAA template but that are primarily relevant to clinical Departments.

**2. Definition of protected health information (PHI):** We define two levels of protected health information based on the type of identifiers that are attached to the information as follows:

**Level 1** PHI may include:

- Names
- Street addresses
- Telephone and FAX numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- License and certificate numbers
- Vehicle identifiers
- Device serial numbers
- URLs
- IP addresses
- Photographs
- Genotype data as defined in section 8A
- Other biometric characteristics that may be used to identify an individual

**Level 2 PHI** only includes:

- Dates of birth and death (except that year is not PHI)
- Admission, discharge, and service dates (except that year is not PHI)
- Dates of procedures and other medical services
- Age 90 or greater
- City of residence
- Zip code

A dataset containing level 2 PHI identifiers but not level 1 PHI identifiers is also referred to as a **limited use dataset**. A dataset will be said to have been “**de-identified**” if health information contained therein is not individually identifiable, that is, if it does not contain any of the identifiers listed above.

### 3. **The security of PHI and of transactions that may contain PHI:**

**A.. The security of electronic datasets containing PHI:** Access to all electronic datasets containing PHI will require the use of a password. All machines containing PHI or with access through the Division network to datasets containing PHI will require passwords to log on. All electronic datasets containing PHI will satisfy the two key requirement (e.g., two distinct passwords, a password and a computer located within a locked office). As an added measure of security, we recommend but do not require that electronic datasets containing level 1 PHI identifiers also be encrypted. When computers that can access PHI are unattended, users will ensure that passwords are required for access using procedures such as logging off, using locking screen savers, or locking their machines with a password. When programs must be run overnight, they will either be run in the background, with the use of a locking screen saver, or using some other mechanism that preserves the necessity for password access. The passwords that provide access to PHI will be available, on a need to know basis determined by principal investigators, to investigators, project managers, database administrators, statistical data analysts, and other members of the research team. When appropriate, individuals outside our Division may be given access to PHI, but only with the explicit permission of the responsible investigator and only if they provide the signed confidentiality agreements that may be required. ID numbers will be the routine approach to identifying subjects, and collaborators will be asked not to provide us with PHI containing level 1 identifiers unless it is necessary. When such data are necessary for a particular project, they will be stored in the smallest possible number of datasets (usually 1), with other datasets within a database being linked to this “master” dataset using ID numbers. Requirements regarding the protection of access to datasets containing PHI apply equally to datasets stored on the network, on desktop computers in the office, on desktop computers at home, and on laptop computers.

**B. The security of floppy disks and other removable media containing PHI:** Floppy disks, CDs, zip disks, tapes containing backups for data on our network, and other removable media which contain PHI must be stored in facilities with at least two different

locks. Ordinarily, this means that they will be stored in a locked filing cabinet/desk within a locked office. When we travel or carry removable media back and forth from home or other off campus locations, access to datasets containing PHI will be password protected and, in the rare circumstances where it is necessary to include level 1 PHI on such media, the dataset will be encrypted. Removable media containing PHI will be physically destroyed when they are discarded.

**C. The security of paper records containing PHI:** Documents and data printouts containing PHI will be stored using the same two-lock principle that applies to removable media. Ordinarily this implies using a locked filing cabinet/desk within a locked office or storage room. When it is to be discarded, printed material containing level 1 PHI identifiers will be shredded. As with electronic media, printed material will ordinarily use ID numbers as identifiers in lieu of names or other level 1 PHI. Collaborators will be asked not to carry or send to us printed materials containing level 1 PHI unless it is essential. Division personnel will not travel with or carry home or to other off campus locations printed materials if it contains level 1 PHI except under strong necessity and with the permission of the principal investigator, the co-principal investigator, or the Director of Consulting Services.

**D. The security of e-mail:** Access to all e-mail is password protected. When we access e-mail from outside the secure network of the Division of Biostatistics, we will use either Secure Socket Layer (SSL) encryption or a Virtual Private Network (VPN) tunnel. Once established, these are usually automated processes that require no action by the user. E-mails containing PHI will be sent to collaborators through secure channels only, and even then, only under strong necessity. Collaborators will be discouraged from sending e-mails with PHI to us and, when it is necessary, they will be asked to send them only through secure channels. Confidentiality agreements will include collaborator commitments to send e-mails with PHI through such channels. E-mails containing PHI will not be stored on a workstation that is not in a secure network.

**E. The security of websites:** In many of its collaborations, the Division of Biostatistics uses websites for such purposes as providing general information to the public, the randomization of subjects, data entry and transfer to and from the Division, and the dissemination of reports. To protect PHI stored on the Web, access will be governed through the combined use of user IDs and role-specific passwords that provide access to selected pages. Web pages containing PHI will be accessed only via the secure server (https) lines. Data entered through the Web reside within our secure network.

**F. The security of home computers and laptop computers:** All home and laptop computers that access the Division network will require passwords to log on. Access to datasets containing PHI that are stored on such machines will be password protected using a password that is different from the one that is used to log on. E-mail connections from home/laptop computers will use an encrypted connection.

**G. The security of FAXes containing PHI:** Unless we are assured by recipients that FAXes will be received in a secure fashion, we will not send FAXes containing PHI.

Collaborators will be asked not to send FAXes with PHI to us unless they are being sent to a private secure office, to an alternative location in which security can be assured, or to a recipient who is alerted first that a FAX is coming so that he/she can physically secure the FAXed document immediately.

**H. The security of passwords:** Each member of the Division is responsible for maintaining the security of his or her passwords. To that end, Division personnel will:

1. Not share passwords with anyone else
2. Not log onto a PHI repository for anyone else
3. Keep written records of passwords under lock and key
4. Change passwords periodically
5. Use passwords that are
  - I) Difficult to guess
  - II) Contain at least six alphanumeric characters

Passwords will be deleted when a user is no longer authorized. Copies of passwords providing access to primary datasets that use password protected encryption will be stored in a locked cabinet in the office of the Division Administrator.

**I. The security of offices and storage rooms containing PHI:** The number of individuals with access to offices containing PHI will be kept to an absolute minimum. Records of who has keys will be maintained under the supervision of the Division Administrator. Individuals who leave the Division of Biostatistics will be required to return their keys. The security of offices during the working day will be maintained through practices that include locking doors and logging off computers (or using other means that require password access) when leaving the office for an extended period, removing documents that contain PHI from visible locations, keeping file cabinets containing material with PHI locked when they are not in use, using video surveillance in hallways outside of offices and, in general, maintaining the same two-key policy during the work day that is required at other times.

**J. Structure of and access to Biostatistics computing facilities:** The Biostatistics computing facilities contains three separate zones.

I) A **public zone** which provides access to users both from inside and outside the Division of Biostatistics contains our mail servers and web servers. The level of security that applies to e-mail and web servers is discussed in sections 3D and 3E. There are no restrictions on who can send e-mails to our servers or on who can access web servers intentionally placed in the public domain. This zone is protected by a firewall that allows limited services on the systems in this domain. Services using plain text passwords such as telnet, ftp, pop3, and imap are disabled.

II) A **private zone** which provides access only to members of the Division of Biostatistics and to designated collaborators includes file servers, print servers, compute servers and personal computers. All

individuals who have access to any component of the private zone, whether or not they are members of the Division of Biostatistics, are required to sign confidentiality agreements. Access to resources within the private zone are restricted to other systems within the private zone which are under our administrative control or via a secure connection.

III) A **student zone** provides students, research assistants, and designated instructional faculty and staff within the Division of Biostatistics with access to specified datasets that are used for instructional purposes. Students will not have access to any component of the private zone unless specialized circumstances apply (e.g., they are research assistants needing access for their job). Rules governing datasets stored in the student zone are discussed in section 7.

**K Confidentiality agreements:** All Division personnel and all students who have access to instructional datasets containing PHI must sign confidentiality agreements. Collaborators may be required to sign confidentiality agreements, with the decision being dependent on the details of the collaborative arrangement and of the data that will be used. Confidentiality agreements will commit the individual to observing all security and privacy procedures that are described in this document.

**L Reporting privacy breaches:** Division personnel who observe privacy breaches or violations of regulations put forth in this document will ideally seek remediation through direct discussion with the involved individual. Alternatively, they should report their concerns to the following individuals, in order of preference:

1. The individual's supervisor
2. The Division Privacy liaison
3. The Division Administrator
4. The Medical School's Privacy Office
5. The anonymous privacy hotline

#### 4. Databases:

**A. Definition of a database:** All data generated by multicenter studies, program projects, and other research projects will generally define a single database. However, if the structure of the data collected by a particular project suggests that the goal of describing the database and the associated access rules would be more conveniently served by defining multiple databases for the project, the PI will have the option to take that approach. For consulting projects, there will be a one-to-one correspondence between consultants and databases, with each consultant having a single database and with all consulting projects overseen by the consultant being a part of that single database. If more than one consultant is assigned to a particular project, one individual will be defined as the "primary" consultant and data for that project will reside in his/her database.

**B. Determining whether protected information is present:** The PI or his/her designee will be the custodian for all databases associated with a given project and will determine who has access to which datasets within each database. The PI will be responsible for determining which datasets contain PHI and for determining the level of the PHI. The PI will also be responsible (1) for either implementing or ensuring that the regulations put forth in this document regarding the storage of electronic and paper documents containing PHI have been implemented and (2) for monitoring the annual registration of each database by the database custodian. The responsibilities described above will apply equally to the databases generated by consulting activities, with the consultant carrying out the required tasks. The Director of Consulting Services for the Division of Biostatistics will oversee these activities for all consulting databases.

**C. The registration of databases:** All databases will be registered and the registration will be updated annually. The registry will categorize databases according to whether they contain level 1 and/or level 2 information, will identify the person who is responsible for making decisions about access to data (usually the PI), will describe the level of security that is being used (e.g., password protected, encrypted), will indicate where the database is stored, and will discuss the rules governing access to data within the database. Registration will be accomplished by completing an online form and the Division Administrator will maintain the registration records. To facilitate the annual update of the database registry, a single calendar date will be determined as the date for updating all databases. An automated e-mail reminder will be sent to all Division personnel one month prior to the date of the annual update.

**D. The structure of consulting databases:** The Director of Consulting Services is usually responsible for assigning consultants to work with clients. Data generated from these consulting projects are stored in large consulting accounts that contain data from several consultants and potentially from many consulting projects for each consultant. Consultants are given access to consulting accounts by the Division's Systems Manager and only the consultants and the Systems Manager have access to those accounts. Within a consulting account, each consultant defines his or her own subdirectories within which data from the consulting projects of the consultant are stored. The consultant will serve as the custodian for his/her own consulting database and will be responsible for registering that database and for the annual update of the registration. The Director of Consulting Services will monitor these activities.

**5. Division responsibilities when collaborators violate security and confidentiality obligations:** Collaborators will be sent PHI by Division personnel only if they have signed a confidentiality agreement, if they are not required to sign confidentiality agreements because their obligation is covered by human subjects agreements, or if the PHI was originally generated by the collaborators own research subjects. However, it is not feasible for the division to take proactive steps aimed at confirming that collaborators carry out their obligations in this regard. Nevertheless, should it come to the attention of a Division staff member that collaborative data are being handled by a collaborator using methods that violate security or confidentiality, we will take proactive steps to encourage

compliance. These steps may include one or more of the following: the staff member discussing the problem directly with the investigator; bringing the violation to the attention of the staff member's supervisor or the Division's Privacy Liaison to pursue discussions with the investigator, discussing the matter with the Washington University Privacy Liaison, using the anonymous compliance hotline and, potentially, terminating the collaborative arrangement.

## **6. Human subject approvals and consent forms:**

**A. Division responsibilities for confirming that collaborators have obtained human subjects approval:** In all research involving human subjects, the Division will obtain and file written confirmation that appropriate Human Subject (IRB) approvals have been obtained or that the project is IRB exempt. If our participation is that of a Coordinating Center or Data Coordinating Center, we will obtain copies of all participating field centers' IRB approvals and consent forms and keep them on file and up-to-date. When we provide consulting services, the client must provide us a copy of the IRB approval or the IRB exemption.

**B. Division response to the absence of human subjects approval:** The Division will not participate in any research project involving human subjects without either documented IRB approval or documentation that the project is IRB exempt. If a consulting client does not obtain approval and is unwilling to do so when requested, the consultant will refer the client to either the Director of Consulting Services or to the Division Administrator. If formal IRB approval has not been obtained for a consulting project, we may consider verbal confirmation by the IRB that approval will be forthcoming at the next IRB meeting as documentation that is sufficient to justify our immediate involvement in the consulting project. Decisions to proceed under these circumstances will require the approval of either the Director of Consulting Services or the Division Administrator. When such decisions are made, a copy of the forthcoming IRB approval will be obtained at the earliest possible date. If we are asked to participate in the planning stage of a research project and the responsible investigator within the division feels that there is ambiguity regarding the need for IRB approval, either the responsible investigator or the Director of Consulting Services will contact the IRB to discuss the circumstances.

**C. Division procedures regarding the time period during which data can be analyzed:** Consent forms signed by subjects on or after April 14, 2003 will include information about the duration of authorized use of data. The consent form may explicitly state that data can be used in perpetuity. Because the IRB has indicated that annual IRB approval carries with it the implication that data collected by investigators during the subsequent year is approved for statistical analysis, the Division will interpret IRB approval as constituting approval to statistically analyze the data.

**D. Revocation of permission to use data:** Research subjects have the right to revoke previously given authorization to use their data. However, HIPAA regulations indicate

that even when permission is revoked, previously collected data may continue to be used if such use is necessary to “preserve the integrity of the study” or if the data are required for the evaluation of the safety of the intervention. Continued use of data under these circumstances only applies to the time frame described in the original consent form. In light of these considerations, Division policy requires compelling reasons to continue to use data in violation of the expressed wishes of a subject who revokes permission. When circumstances suggest that such action might be appropriate to preserve the integrity of a study or to evaluate the safety of the intervention, the following case by case procedures will apply. If our Division is collaborating with outside institutions, the Principal Investigator within the Division will bring the matter to the attention of Washington University’s IRB. If it is a collaboration or consulting project within Washington University, the IRB will be consulted about the matter by an investigator outside the Division, by the responsible investigator within the division, or by the Director of Consulting Services for the Division of Biostatistics, depending on which individual is deemed most appropriate for the particular project. The Division will not analyze data when permission has been revoked by a subject unless such action has been sanctioned by the Washington University IRB. Records of all subject revocations will be maintained within our Division by either the responsible investigator or the consultant.

**E. Data use agreements:** Collaborators will not be required to sign data use agreements because IRB approval will constitute approval to analyze data for the period during which the approval is in force. Data use agreements will be obtained before data with PHI are distributed to interested parties who are not participating in a study as collaborators.

**7. Datasets used for instructional purposes:** All HIPAA regulations that apply to data used for research purposes apply in the same way to data that are used for instructional purposes. Thus, we will only use data containing PHI for instructional purposes if the consent form either explicitly or implicitly permits such use within the relevant time frame. If the appropriate informed consent is not available, data will be used for instructional purposes only if it has been de-identified in compliance with HIPAA regulations and procedures discussed herein. If PHI is included in instructional datasets, all procedures discussed in this document regarding electronic security and the handling of printouts generated by the data must be followed. All students, faculty and staff who have access to instructional data containing PHI must sign confidentiality agreements.

## **8. Genetic data:**

**A. Genotype data:** Genotype data will be routinely treated as PHI. In some circumstances, some datasets may contain only a few common genetic variants or such little genotype data that the risk of identifying individuals is small. In this case, researchers may request the standard waiver of an independent statistician certifying that the risks of identification are small. But in the absence of such a waiver, we will treat genetic information as PHI

**B. Pedigree structure:** In and of itself, we do not consider pedigree structure information to be PHI. Every individual has exactly one father and one mother (whether or not they are alive or identified). Even extremely large family sizes will not uniquely identify an individual especially as the size of the dataset grows and the number of field sites increases (as is typical in family studies). Thus, if data from the individuals within a pedigree are de-identified in accordance with HIPAA regulations, the pedigree itself has also been de-identified and does not constitute PHI.

**9. Access by individuals to Protected Health Information:** Our Division does not generally have access to the medical records that are the likely source of requests for access. If access to our research data is requested, we will refer the request to the PI responsible for acquiring the original health information. If asked to do so, we may act as an agent of the PI..

**10. Accounting for Disclosures of Protected Health Information:** Our Division does not generally have access to the medical records that are the focus of this Template. Nevertheless, should circumstances arise where we are involved in the Disclosure of PHI for any reason, we will observe the procedures outlined in Template # 3 of Washington University's HIPAA guidelines.

**11. Amendment of Protected Health Information:** Our division does not generally have access to the primary health records that are the likely sources of requests for amendment. If we are asked by subjects to amend data in our custody, we will refer the request to the PI responsible for acquiring the original health information. If we are asked to do so, we may act as an agent of the PI.

**12. Authorization for use or disclosure of Protected Health Information:** A dataset containing only level 2 PHI (i.e., a limited use dataset) can be used or disclosed for research purposes without an authorization or waiver of authorization when an appropriate data use agreement has been signed. The signing of an appropriate consent form combined with IRB approval constitutes authorization to use or disclose all PHI for research purposes.

**13. Use or disclosure of Protected Health Information with Business Associates:** Ordinarily, the only individuals to whom our Division discloses PHI are collaborators who have committed themselves to observing the guidelines put forth in this document. Should circumstances arise where it might become necessary to disclose PHI to Business Associates (e.g., consultants or attorneys), we will not commence such disclosure until the Business Associate provides us with two copies of a Business Associate Agreement. Also, we will develop a review mechanism that is specific to the particular Business

Associate and that ensures that the disclosure of PHI is consistent with Washington University and Division of Biostatistics HIPAA policies. Unless it is essential, we will not disclose level 1 PHI to Business Associates.

**14. Appropriate methods of communicating Protected Health information:**

Ordinarily, the communication of the PHI to which our Division has access occur only in the context of our research activities. We are not involved in discussions with patients, family member, or friends. Earlier sections in this document have discussed both our procedures for ensuring privacy when we communicate research data with collaborators and for disclosing PHI to potential Business Associates.

**15. Use or disclosure of PHI in fundraising:** Our Division has not previously been involved in fundraising activities where the use or disclosure of PHI was an issue. Should this become an issue in the future, our policy is that we will, at most, disclose summary data that does not constitute PHI.

**16. Use or disclosure of PHI in marketing:** Our Division has not previously been involved in marketing activities where the use or disclosure of PHI was an issue. Should this become an issue in the future, our policy is that we will, at most, disclose summary data that does not constitute PHI.

**17. Use or disclosure of PHI in media relations:** Our Division has not previously been involved in media related activities where the use or disclosure of PHI was an issue. Should this become an issue in the future, our policy is that we will, at most, disclose summary data.

**18. Minimum necessary request, use or disclosure of Protected Health Information:** Unless it is necessary, it is our standard policy to ask collaborators not to provide us with level 1 PHI. Similarly, it is our policy not to disclose level 1 information to collaborators unless it is essential. In general, our policy is to have access to and to disclose the minimum necessary level of PHI. In stating this policy, we note that the minimum necessary rule does not apply to “research that includes treatment”, a type of research activity that constitutes a substantial portion of our activities.

**19. Distribution of notice of privacy practices:** Our Division does not generally have direct contact with patients and therefore does not have the opportunity to distribute notices of privacy practices.

20. **Use or disclosure of Protected Health Information without a verbal or written agreement:** The only PHI to which our Division ordinarily has access are research data provided to us under the auspices of written or verbal consent. Should we be requested through some legal or other procedure to disclose PHI without agreement, we will discuss the matter with the Washington University Privacy Office, the Office of General Counsel, or with the Risk Management Office and will proceed accordingly. If it becomes necessary for us to disclose PHI without verbal or written authorization, we will complete the relevant disclosure form to documents the details.

21. **Use or disclosure of psychotherapy notes:** Our Division does not have access to psychotherapy notes and there is no prospect that we will have such access in the future.

May, 2003