Table of Contents

1. Revision History ........................................................................................................................................... 2
2. Policy ............................................................................................................................................................ 2
   2.1. Overview .............................................................................................................................................. 2
   2.2. Confidentiality ..................................................................................................................................... 2
   2.3. Requests for Information ....................................................................................................................... 5
      2.3.1 Internal Requests .......................................................................................................................... 5
      2.3.1 External Requests .......................................................................................................................... 6
   2.4. Disposal of Information ......................................................................................................................... 7
   2.5. Enforcement ......................................................................................................................................... 7
3. Related Documents ......................................................................................................................................... 7
4. Appendix ...................................................................................................................................................... 8
1. Revision History

<table>
<thead>
<tr>
<th>Revised by</th>
<th>Approved By</th>
<th>Approved by Signature</th>
<th>Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tamara Britt</td>
<td>Terry Callaghan</td>
<td>11/16/2015</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Policy

2.1. Overview
The Rutgers University Foundation Information Technology Department ("RUF-IT") maintains data concerning Rutgers, the State University of New Jersey's ("Rutgers" or "Covered Entity") donors, alumni and other constituents (the "Data" or the "Database") for the Rutgers University Foundation ("RUF" or the "Foundation"). All information contained in it the Database is confidential and may be used only for appropriate Foundation, Alumni Relations and University purposes by Foundation workforce, which includes Foundation, RUF-IT and Alumni Relations employees and volunteers ("Foundation Workforce"), in accordance with this policy on confidentiality and release of constituent information ("Confidentiality Policy").

2.2. Confidentiality
Access to the Data will be provided only to Foundation Workforce members who have an appropriate business need for such access. Each Foundation Workforce member who has been granted access to the Data is responsible for maintaining the confidentiality of the information and must take precautions to ensure that such information is not disclosed to any person other than in connection with the Foundation, Alumni Relations or University purposes for which it has been provided. Data may not be distributed or used for personal, commercial or political gain. Any Foundation Workforce member who is granted access to the Database must have read the Acceptable Use Policy sign a “System Access Form” that explains the Account Usage Policy.

Except as provided in the Confidentiality or Account Usage Policies, the Foundation prohibits the release of student and alumni social security numbers and other private information to any third party without that student or alumni’s written consent.
Certain Data are considered Personal Identifying Information (“PII”) or Personal Health Information (“PHI”), as described herein. PII and PHI are subject to federal and state privacy protection and must be treated with extra caution. PII refers to information that can be used to uniquely identify a single individual, for example, name plus birth date, social security numbers, credit card numbers, driver’s license numbers, and cell phone numbers. This data may not be stored on personal computers, laptops, shared or network drives, mobile devices, portable storage devices or the like, or transmitted electronically in any form, including by email. The Federal Family Education and Privacy Rights Act, 20 U.S.C. 1232g, prohibits the release of student and alumni social security numbers to any third party without the individual’s consent.

PHI is “individually identifiable health information” that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium, but not including individually identifiable health information stored in education records covered by the Family Educational Rights and Privacy Act, as amended, records described at 20 U.S.C. 1232g(a)(4)(B)(iv), employment records held by a Covered Entity in its role as employer, or regarding a person who has been deceased for more than 50 years. “Individually identifiable health information” includes demographic information collected from an individual and is information that is created or received by a health care provider, health plan, employer, or health care clearinghouse; relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Please contact the Foundation’s Associate Vice President of Information Technology if you are involved in a project that may require the release of any PII or PHI data outside of the Foundation. Release of any PII data involving alumni, parents, students, faculty or staff must be reviewed and approved by legal counsel.

Any Foundation Workforce member making a request for a report or data file for a mailing must exclude from the mailing constituents who have requested not to receive mail, are indicated as “do not contact under any circumstance” or who have other mail contact exclusions, including those who opt out of the use or release of their Personal Health Information as described below. Approved HIPAA opt out language can be found in the Foundation Collaboration Center. Please refer to the user manuals or contact the IT help desk for the latest set of exclusion codes.
The Foundation, including Alumni Relations, does not create Personal Health Information ("PHI"), which is defined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended, and its implementing regulations. However, from time to time the Foundation may receive from the affiliated Covered Entity organizations to which it is institutionally-related, including but not limited to: Graduate School of Biomedical Sciences, Rutgers School of Dental Medicine, New Jersey Medical School, Robert Wood Johnson Medical School, Cancer Institute of New Jersey, Ernest Mario School of Pharmacy, Center for Advanced Biotechnology and Medicine, Environmental and Occupational Health Sciences Institute, School of Health Related Professions, Rutgers School of Nursing, Rutgers College of Nursing, School of Nursing – Rutgers Camden, School of Public Health, Robert Wood Johnson University Medical Group, University Behavioral Health Care, Institute for Health, Health Care Policy and Aging Research certain limited PHI permitted for conducting fundraising activities on behalf of the Covered Entities, in accordance with HIPAA, ("Fundraising PHI"). Fundraising PHI includes only:

- Patient demographic information (e.g., name, contact information, birthdate, age and gender)
- Health insurance status (e.g., whether someone is insured and the type of insurance)
- Dates of care/services
- The department that provided the care (e.g., oncology, etc.)
- Information about the treating physician(s)
- Outcome information (e.g., the death of the patient, or that the surgery was successful or any sub-optimal result of treatment or services)

**Note:** Information concerning diagnosis, prognosis or the nature of services or treatment provided is PHI but is not considered to be Fundraising PHI.

Fundraising PHI is subject to federal privacy protection under HIPAA. Foundation Workforce members will use and disclose Fundraising PHI only as permitted by HIPAA and New Jersey law. Foundation Workforce members may not use, create or disclose any PHI and may not accept any PHI from or on behalf of a third party, including those affiliated with the Foundation, other than Fundraising PHI (the proper use of which is discussed below). Further, Foundation Workforce members should take care not to include health information volunteered to them by donors or prospects in their contact reports and notes entered into the Database and shall protect the
Confidentiality of such information that may be disclosed to them in accordance with RUF prospect management training and the Confidentiality Policy.

Any PHI received by Foundation Workforce members from a Covered Entity other than Fundraising PHI and any violation of RUF prospect management training and the Confidentiality Policy should be reported immediately to the Foundation’s President, Vice President of Alumni Relations or Associate Vice President of Information Technology.

Foundation Workforce members may receive, use and disclose Fundraising PHI only within the Foundation, including Alumni Relations, only in accordance with RUF prospect management training and the Confidentiality Policy and only to the minimum extent necessary to carry out the charitable and fundraising mission of the Foundation. If the Foundation must work with or engage an outside vendor to perform fundraising activities using the Fundraising PHI disclosed to it by a Covered Entity, a Business Associate Agreement between the applicable Covered Entity and the vendor must be in place prior to any use or disclosure by the Foundation to the vendor. Please contact the Foundation’s Associate Vice President of Information Technology if you are involved in a project that may require the release of any PHI outside of the Foundation for fundraising purposes.

2.3. Requests for Information

2.3.1 Internal Requests

Requests for reports, electronic files or other information from the Database must be submitted as an IT Project Request in the Foundation Collaboration Center. The form must include a description of the purpose for which the data is being used.

Requests for data from a University staff member from outside the Foundation Workforce must be approved by the dean, development officer or alumni relations officer for that school or unit. Gift data can only be released with the approval of the dean or development officer. The request should be submitted by the development officer or alumni relations officer as an IT Project Request via the Foundation Collaboration Center.

Prospect and wealth data can only be released with the approval of a Vice President or President of the Foundation. These requests should be sent by the VP/President via email to the AVP, Information Technology.

Foundation Workforce members who create reports from the system may share this information with other University staff for appropriate Foundation, Alumni Relations or
University purposes, but only if the staff member receiving the data has signed an RUF-IT confidentiality statement within the past twelve months. In addition, each file or report must have attached the “Acceptable Use Statement – Confidential Donor and Alumni Information.” All signed confidentiality statements must be forwarded to the Foundation IT Department for recording.

2.3.1 External Requests

Information from the Database may only be released to law enforcement officials, government agencies or other third parties with the written approval of the Foundation’s President. In his/her absence, if the release of data is pressing and cannot wait, the approval may be made by the Vice President of Alumni Relations or Associate Vice President of Information Technology. A written request must be made on the requester’s letterhead and the identity of the requester must be verified. A valid subpoena may be required as well. Any release of donor information must also be coordinated through Donor Relations.

Information from the Database may not be released to classmates, friends, relatives or other individuals who are trying to contact alumni or other constituents. An alumnus requesting contact information for another alumnus should be directed to the online directory system. Contact information for those alumni who have opted out of the online directory system should not be released. Alumni directories, both in paper and electronic format (e.g., website, CD) are solely intended to facilitate personal contact between alumni. Use of these directories for large-scale mailings or other mass communications of any kind, or for any other commercial or political purpose, is prohibited.

The Foundation’s President, Vice President of Alumni Relations and Associate Vice President of Information Technology have the authority to release information other than PHI to third parties who are working on behalf of the Rutgers University Foundation or the University. This includes, for example, directory publishing companies, research firms and merchandise vendors. The vendor or consultant must agree to use the information only for the purpose intended by the Foundation or the University and must sign a confidentiality agreement. PHI shall not be disclosed to a third party except in accordance with a Business Associate Agreement between the applicable covered entity and the third party. The vendor is prohibited from selling or transferring any of the information it receives from the Database.

Requests for release of information to volunteer alumni constituent groups must be approved by the Foundation’s President, Vice President of Alumni Relations or Associate
Vice President of Information Technology. The released information must be limited to information concerning those alumni who are affiliated with the requesting group (e.g., information about Glee Club members can only be released to alumni who are affiliated with the Glee Club). Except in extraordinary circumstances and approved by the Foundation’s President, the information shared will be limited to directory and summary level giving data. The use of this information by the constituent groups must be monitored by a Foundation or Alumni Relations staff member. The employee who monitors the request is responsible for determining the intended use, verifying that the users adhere to the Confidentiality Policy and ensuring that they have signed the appropriate confidentiality agreements or a Business Associate Agreement is in place, if necessary.

All requests for information from members of the media must be referred to the Alumni Relations and Foundation Communications Department.

All requests for information under the NJ Open Public Records Act (OPRA) must be coordinated through the Foundation’s President and the University Records Custodian, Office of the University Secretary.

Donors have the right to remain anonymous if they do not want their Database information published. Please see IT and Records policies for more information.

In cases of dispute about whether information should be released, the final decision will rest with the Foundation’s President.

2.4. Disposal of Information
All electronic media, including tapes, diskettes, CDs, memory cards, thumb drives, and the like that contain donor, alumni or constituent information shall be returned to IT after use so they can be destroyed appropriately. All printed material that contains donor, alumni or constituent information shall be shredded.

2.5. Enforcement
Failure to abide by the Confidentiality Policy could result in disciplinary action up to and including termination, and other legal action, including those seeking damages resulting from the violations and injunctions against future violations.

3. Related Documents

- “Acceptable Use” – Policy
4. Appendix

N/A
By signing below, I certify that:

1. I have received a copy of the Policy on Confidentiality and Release of Constituent Information ("Confidentiality Policy") of the Rutgers University Foundation (RUF).

2. I have read and understood the Confidentiality Policy, and I agree to abide by its terms and conditions, some of which include:
   - Maintaining the confidentiality of RUF and Rutgers University Alumni Association (RUAA) information and not sharing any RUF and/or RUAA information with people who have not signed the Confidentiality Policy
   - Not storing Personally Identifiable Information (PII) or Personal Health Information (PHI) on any personal devices (e.g. names, addresses, birth dates, Social Security numbers, etc.) – see “Information Classification” Policy for full definitions
   - Not releasing any PII or PHI to an entity that does not have a Business Associates Agreement on file
   - Not sending mail or solicitations of any kind to those that have elected not to receive them
   - Properly using the Foundation Collaboration Center to submit reports and information requests
   - Properly disposing of RUF and/or RUAA information when necessary
   - Never sharing any of my account passwords with anyone, including the RUF Help Desk
   - Reporting any violations of the Confidentiality Policy to Management

3. I acknowledge that all materials and information prepared and received by me as a part or consequence of my work with the RUF and/or RUAA are the property of the RUF and/or RUAA, regardless of whether they are in paper, electronic or other form.

4. I agree to return all confidential materials and information in my possession at the end of my employment or change in volunteer status/position with the RUF and/or RUAA.

5. I understand that my obligations under this policy will continue after the termination of my employment or volunteer assignment with the RUF and/or RUAA.

6. I acknowledge that I must read and sign this form annually to maintain access.

Print Name: ___________________________  School Department: ___________________________

Signature: ___________________________  Date: ___________________________