|  |
| --- |
| State Health Plan Data Request |
| **Civil Money Penalties.**  Office of Civil Rights may impose a penalty on a covered entity for a failure to comply with a requirement of the Privacy Rule.  Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity’s failure to comply was due to willful neglect.  Penalties may not exceed a calendar year cap for multiple violations of the same requirement.

|  |  |  |
| --- | --- | --- |
|  | **For violations occurring prior to 2/18/2009** | **For violations occurring on or after 2/18/2009** |
| **Penalty Amount** | Up to $100per violation | $100 to $50,000 or moreper violation |
| **Calendar Year Cap** | $25,000 | $1,500,000 |

**Criminal Penalties.**  A person who knowingly obtains or discloses individually identifiable health information in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one-year imprisonment.  The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to 10 years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use identifiable health information for commercial advantage, personal gain or malicious harm.  The Department of Justice is responsible for criminal prosecutions under the Privacy Rule. |
| Organization |
| 1. Name of Organization:
2. Research Affiliation: (University, Medical Center, n/a):
3. Primary Contact Name/Phone/email:
4. Alternate Contact Name/Phone/email:
5. HIPAA Compliance Contact Name/Phone/email:
6. Date of Request:
7. SHP Business Owner:
 |
| Request Type |
| Use: (TPO/Research/Other)Data: (Identified, De-identified, Limited Data Set, Aggregate) |
| Request Description |
| Describe the request for data. Identify the intended use of the data and outcomes. Please attach any documentation which may assist in the understanding the project for which you are requesting the data. If you have you obtained an IRB waiver of authorization, please attach a copy. If PHI is being requested, describe why PHI is necessary for this request. Explain how minimum necessary rule has been applied. |
| Please Complete the Following Section ONLY if You Are Requesting PHI |
| Security Measures |
| 1. Is HIPAA training mandatory for all employees or only those employees who use, disclose or have access to PHI?
2. Are HIPAA policies and procedures in place for employees to follow, are they trained on the policies and procedures, and are they required to sign an agreement stating they have read and understand the policies and procedures?
3. Provide the names of employees and their positions associated with this project, who will have access to PHI. (If necessary, please complete and attach an additional page.)
4. Where will SHP data/PHI reside within your organization (i.e., personal computers, workstations, USB drives, networks, server(s), software applications, member/customer portals, and other mobile devices)?
5. Provide details of the methods your organization utilizes for securing and rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals.
6. Will you be utilizing a subcontractor for this project? If so, do you have a Business Associate Agreement (BAA) with that organization?
7. Please provide detailed documentation regarding the number of HIPAA breaches incurred within the past five (5) years. Details of each breach, *if any*, should include: date breach occurred; number of individuals affected; cause of the breach (e.g., stolen or lost laptop; unsecured or unprotected server, laptop, or facility, etc.); method for informing affected individuals; and how the breach was mitigated.
 |
| Signature |
| Your signature below indicates your understanding of your responsibilities for safe guarding this data. It also confirms your understanding this data cannot be shared without explicit approval of the Department of State Treasurer, State Health Plan Division. In addition, by signing this document, you acknowledge that if you receive PHI as defined under HIPAA, you have the necessary and appropriate safeguards in place to protect such information, that employees using the information have been properly trained in the use and protection of PHI and that policies and procedures exist surrounding the creation, receipt, maintenance, or transmission of the PHI.Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Print\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Internal Use Only |
| 1. Has this request been reviewed by DUDC committee members?
2. Has a BAA/DUA been signed? If not, why not?
3. Has legal approved this request?
4. Has the cost to the Plan been evaluated?

Date of Approval: SHP authorization signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |