Guide to Responding to Inquiries, Complaints & Access Requests

The Privacy Policy: Individual Rights requires each department to assist individuals in protecting their privacy and in exercising their rights under the Privacy Policies. This means that inquiries and access requests must be responded to appropriately and complaints must be taken seriously and treated diligently.

1. Responding to Inquiries

If an individual has a question about our handling of personally identifiable information (PII), start by providing the individual with a copy of the applicable privacy notice. In many cases, answers to privacy-related questions can be found by reading the notice. For example, if the individual wants to know why you are asking for PII, that information will be in the notice. The notice will also explain what rights the individual has and how to exercise those rights.

If the individual has a question that is not answered by the notice, document the question. If you are certain of the answer, you can provide it to the individual. Also send an email to the department privacy officer about the question. Your privacy officer needs to know what questions people have that are not covered by the notice. It might be necessary to update the notice.

If you are not certain of the answer to the person's question, tell the individual that you will have to ask your manager or the department privacy officer. Either you should report the answer back to the person or confirm that your manager or the privacy officer will respond directly to the person with the answer. Each worker is responsible for confirming that the matter is resolved.

2. Handling Complaints

Each department should establish a process for submitting complaints to the privacy officer. The following steps can help streamline this process:

- Develop a method for capturing complaints in writing, using a standardized reporting form. The form can be sent to the privacy officer (or his/her designee) via email to a designated address.

- Ideally the person making the complaint should fill out the form. However, in some cases an individual may submit a complaint orally (such as over the telephone) or else the person may be unwilling or unable to complete the form. In these situations, the worker receiving the complaint should see that it is documented in writing and forwarded to the privacy officer.

- Employees may also report violations to their own managers or to other executives in the relevant business unit.

- Privacy notices should include contact information for individuals to use when submitting complaints or questions.

- Once a complaint is received by the privacy officer, an acknowledgement of receipt of the complaint should be sent to the complainant.

- Whenever a complaint or request involving privacy rights is made, the privacy officer should examine it in the context of applicable law and the Executive Branch Privacy Policies to determine if the request is justified.

- All complaints and requests should be dealt with in the strictest confidence.

- Communications and notifications to the complainant should (where possible) be made in writing. They may be made in the same way that the original complaint was made (*e.g.*, via email, letter or fax).

- Complaints and inquiries will be resolved without cost to the individual.

- The privacy officer should normally respond to the complainant with a decision as to the request or complaint within seven days. When this is not feasible because of the complexity of the matter or other reasons, the complainant should at least be contacted within seven days and be told when he/she can expect a final decision.

- Complaints must be logged and reported monthly to the Executive Branch Chief Privacy Officer. In the event of a serious compliant or threat of litigation, the Chief Privacy Officer should be notified immediately. Legal counsel may also need to be engaged.

Investigation of the Complaint

- The privacy officer may investigate a complaint personally or to assign responsibility for all or part of the investigation to another manager (such as a department manager or an OT manager). The privacy officer remains responsible for ensuring that the investigation is handled properly.

- The investigation may be conducted in any reasonable manner. At a minimum, however, if the complaint suggests that there may have been a violation of a Privacy Policy or the law, the person(s) involved will be asked to reply to the complaint.

- At the discretion of the privacy officer, the complainant may be re-contacted to provide more information or to respond to statements made by others in the course of the investigation.

- If the privacy officer finds that indeed there has been a violation of a Privacy Policy or law, he/she will recommend appropriate remedial action. If the official concludes that the violations of the Privacy Policy or law were serious or willful, the privacy official may decide also to initiate appropriate disciplinary action in accordance with the Accountability Policy.

- When the investigation has been completed, the complainant will be informed, in general terms, of the results of the investigation and of any remedial action, if any, that will be taken.

- If the outcome of an investigation demonstrates that certain PII processing practices need modification, this must be promptly reported to the Chief Privacy Officer so that adequate action can be taken.

Non-binding Nature of these Procedures

These rules and procedures provide general guidance for the handling of privacy-related complaints. They are not intended to be binding. Workers and other individuals do not have any legally enforceable rights pursuant to any of these rules and procedures. They may not invoke any such rules and procedures in any legal proceedings or with respect to any claims.

3. Responding to Access Requests

The Privacy Policy: Individual Rights recognizes that individuals have the reasonable right, upon request, to learn whether a department maintains personal information about them and to view the personal information held.

Access rights are not unlimited. Unless access rights are mandated by law (such as FOIA), access and/or correction may be denied where (i) the costs of providing access are unreasonable given the possible benefit to the individual, (ii) providing such access or correction could compromise the privacy of another person or unreasonably expose sensitive information, or (iii) access would be contrary to other department policies that restrict access.

- Workers can generally exercise their access rights using the HR Self-Service Application or by contacting their human resources managers.

- Other individuals who wish to exercise their rights of access shall do so in writing. (To facilitate access, each department should have a form that individuals can use to submit the requests.)

- Charges imposed upon individuals for access must be reasonable. The privacy officer must approve access fees.

- All individuals must provide appropriate proof of identity prior to being granted access.

- Upon provision of the request form and identification, the department shall:

    - Determine if it maintains accessible information about the individual,

    - Provide the individual with a completed access report, in the form attached here or another similar form,

    - Provide the individual with information on how to update or correct the personal information. and

    - Provide the individual with contact information for the department privacy officer.

- Consistent with legal requirements, departments may deny any access requests that are frivolous or harassing, such as repeated access requests over a short period of time.