

Privacy Impact Assessment Long Form Supplementary Questionnaire

Business Related Questions

11. Does HHS own this system?

If no, identify the system owner.

12. Does HHS operate the system?

If no, identify the system owner.

13. Is this system new or existing?

14. Is this system in development or production?

19. How are personal records retrieved? In other words, what search/filters can be applied to bring up personal information on an individual?

22. Does this system share or disclose personal information with any other divisions within HHS, external agencies, or other people/organizations outside the agency?

If so, what personal information is shared?

23. If the system shares information please specify with whom and for what purposes.

24. Is the personal information in the system used to retrieve data in other systems?

25. Is there a process in place to notify organizations or systems that are dependant upon the personal information contained in the system when major changes occur (revisions to personal information, or when the system is replaced)?

26. Are individuals notified how their personal information is going to be used?

If yes, please describe the process for allowing individuals to have a choice.

28. Are there processes in place for periodic reviews of personal information contained in the system to ensure the integrity, availability, accuracy and relevancy?

If yes, please describe the process.

29. Are there rules of conduct in place for access to personal information?

Please identify which users have access to personal information, and the purpose for that access:

Categories	Yes/No
Users	
Administrators	
Developers	
Contractors	
Other (Who?)	

30. Please describe in detail the information the agency will collect, maintain, or disseminate personal information and why and for what purpose the agency will use the information. In this description, indicate whether submission of personal information is voluntary or mandatory:

31. Please describe in detail any processes in place to:

- notify and obtain consent from the individuals whose personal information is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection),
- notify and obtain consent from individuals regarding what personal information is being collected from them and how the information will be used or shared

38. If the system has a website, does it collect personal information from individuals?

39. Are rules of conduct in place for access to personal information on the website?

48. If contractors operate or use the system, do the contracts include clauses ensuring adherence to the privacy provisions and practices?

Technical Questions

8. Please provide the physical location (street address) of the system server(s):

If the system hosts a website (includes web apps) please answer questions 33, 34, 35, 36, 40

33. Is the website accessible by anyone other than NIH (this would include 3rd party developers/administrators)?

34. Is a website privacy policy statement (consistent with OMB M-03-22 and Title II and III of the E-Government Act) posted on the website?

35. Is the website's privacy policy in machine-readable format, such as Platform for Privacy Preferences (P3P)?

36. Does the website employ persistent tracking technologies?

Categories	Yes/No
Web Bugs	
Web Beacons	
Session Cookies	
Persistent Cookies	
Other (if so what?)	

NIH ORS and ORF Privacy Impact Assessment
Long Form

40. Does the website contain links to sites external to the NIH?

If so, is there a disclaimer notice that indicates the user is now leaving NIH?

43. Is there a contingency (or backup) plan for the system?

44. Are files backed up regularly?

45. Are backup files stored offsite?

46. Are there user manuals for the system?

49. Are methods in place to ensure least privilege (i.e., “need to know” and accountability)?

If yes, please specify method(s)

51. Are technical controls in place to minimize the possibility of unauthorized access, use, or dissemination of the data in the system?

If yes, please identify which technical controls are currently in place:

Category	Yes/No
User Identification	
Passwords	
Firewall	
VPN	
Encryption	
IDS	
Common Access Cards	
Smart Cards	
Biometrics	
PKI	

NIH ORS and ORF Privacy Impact Assessment
Long Form

53. Are physical access controls in place to protect the system?:

If yes, please identify all physical controls that are currently on the system:

Categories	Yes/No
Guards	
Identification Badges	
Key Cards	
Cipher Locks	
Biometrics	
CCTV	