Version updated: 8 February 2023
Compiled by the NAACCR Data Security & Confidentiality Workgroup

Requests from or on behalf of Patients for Individual-Level Information from Central Cancer Registries

Editors:

Bozena M. Morawski, Cancer Data Registry of Idaho

Recinda Sherman, North American Association of Central Cancer Registries

Jean-Michel Billette, Canadian Cancer Registry – Statistics Canada

David Chesnut, Information Management Services, Inc.

Castine Clerkin, North American Association of Central Cancer Registries

Steven Friedman, National Cancer Institute, National Institutes of Health

Susan Gershman, Massachusetts Cancer Registry

Selina Khatun, Nunavut Cancer Registry

Lauren Maniscalco, Louisiana Tumor Registry

Robert McLaughlin, Cancer Registry of Greater California

Qianru Wu, Nebraska Cancer Registry

Heather Zimmerman, Montana Central Tumor Registry

Publication date [1] : October 30, 2022

[1] These guidelines should be reviewed and updated every 12 months.

Table of Contents

Background

Central cancer registries receive requests for information about specific individuals reported to the registry with a reportable cancer. These requests may be from the patient, the patient's family, or other entities (e.g., attorneys).

Requests arise for many reasons, including but not limited to, compensation under federal programs (e.g., The Radiation Exposure Compensation Act[2]), to get information regarding their own health record (particularly for childhood cancers), to obtain additional information about their family history of disease, or for continuity of care.

Purpose

This document aims to provide information about the role of a central registry when responding to these types of inquiries. Central cancer registries only maintain a small portion of a patient's cancer related data. **However, there are instances where a central cancer registry would like to provide patient-specific information to a patient or a patient's family or representative.**

Cancer surveillance and legislation guiding patient data release can change frequently, so always ensure your registry understands all relevant legislation and policy. As with any data request, state cancer registries must be knowledgeable of their specific state or local laws and institutional policies/regulations regulating the regarding release of protected health information (PHI) held at the registry to members of the public.

Recommended Practices for Central Cancer Registries When Responding to Requests

The below describes recommended practices for responding to these requests.

[2] https://www.justice.gov/civil/common/reca; https://sgp.fas.org/crs/misc/R43956.pdf

Ensure Adherence to Best Practices: Know Your Registry's Policies and Procedures and Applicable Statute

The below questions are designed to help registries identify which federal, state and local laws and institutional regulations they are bound by when responding to data requests from individuals for patient-specific data. In addition, answering these questions is intended to ease the data compilation and provision process.

• Is your registry located in a HIPAA-covered entity? (Most central registries will not be HIPAA-covered entities. However, if you are a HIPAA-covered entity, follow your organization's HIPAA-specific policies and procedures.)
• What do the laws and regulations covering your registry say about patient level data release? Is there a specific statute mandating data release to requestors?
• Does your registry have specific policies and procedures around patient-specific data release to individuals?
• Have you determined that registry data is the most appropriate data for the requestor's use case?
• Have you confirmed that the requestor has the legal authority to obtain requested data?
• Have you verified the data elements required for the requested use case?
• Have you determined that the requested/required data elements are releasable without additional authorization from providing entities, e.g., vital statistics data?
• Have you determined and received documentation from the requestor of where and how to transmit requested data?
• Has this request been logged at your registry?

Guide the Requestor to the Best Source of Information

If the patient or representative requires clinical records, the central registry should recommend that the requestor contact the healthcare provider or other entity that they have a relationship with to obtain this information, e.g., their healthcare provider. Healthcare providers or other HIPAA-covered entities generally have the most complete record of a patient's cancer and a standard records release

protocol. Other examples of entities with data on a patient's cancer include health insurance companies or health programs that they have participated in.

If the requestor is unable to get the required information from a healthcare provider or other source, the central registry may wish to provide data to the requestor. This may be the case if the patient's medical record is destroyed, archived or otherwise unavailable, or if they are looking for a long-term summary, as is often the case for pediatric cancer survivors.

Confirm that the Requestor Has Legal Authority to Obtain Data

If the central cancer registry wishes to provide data to the requestor, registries should first confirm that the requesting party has the legal authority to request data on the specific patient in question. Note: there may be specific agreements, policy, or legislation that prohibits your registry from releasing various types of data for specific purposes. ***Knowledge of your state/local laws and registry policies/agreements are critical to ensuring that the appropriate data are released to a requestor.***

- If the patient is requesting their own data, proof of identification must be requested and authenticated, e.g., witnessed by an appropriate party or notarized. Appropriate witnesses may be identified per state/local statute. A signed authorization from the individual allowing the release of their data should be requested. (See Appendix A.)
- If data are requested for a deceased patient, a copy of the death certificate and documentation establishing the requesting party as the patient's designated personal representative or the legal executor of the estate must be requested and authenticated, e.g., witnessed by an appropriate party or notarized. Appropriate witnesses may be identified per state/local statute.
- If data are being requested by a third party for a patient that is not deceased, documentation establishing that requesting individual as a legal Authority for the patient (e.g., parent of the minor patient, Power of Attorney, consent in a class action suit) must be requested and authenticated, e.g., witnessed by an appropriate party or notarized. Appropriate witnesses may be identified per state/local statute.

- For all of the above, specific information detailing where the information should be sent (e.g., physical address, email address) should be provided by the authorized requesting individual.

For a template for requests for Personal Health Information is included in Appendix A.

Establish a Policy on which Data to Release

Depending on the use case for requested data, different data elements may be required to meet the needs of the requestor. As discussed above, the ability to release data is governed by specific state or local laws and institutional policies/regulations. Further, provided that data release generally is permissible, the ability to release specific data items may also be subject to specific state or local laws and institutional policies/regulations – in particular, agreements with other state or local agencies, i.e., vital statistics. Depending on your registry, this may be the entire abstract or only date of diagnosis, primary site, histology and stage.

Compensation for Work Required to Compile Requested Data

Registries may choose to collect payment from a requestor if the information being requested requires a particularly burdensome amount of personnel time, e.g., consolidation of source records into a different form than registry standard.

Relevant Federal Legislation

The Health Information Portability and Accountability Act (HIPAA) – United States

The provision of patient-specific information by a central cancer registry to a member of the public is not an activity that is covered under HIPAA. HIPAA applies to Covered Entities, i.e., those institutions that are health care providers and transmit health information in an electronic form. Most central cancer registries are not considered Covered Entities under HIPAA, and therefore are not required by the HIPAA Privacy Rule to disclose PHI to individuals. (There are some instances where central cancer registries are housed in HIPAA-covered entities, which may affect the registry's policies on data release.) Central cancer registries may, however, provide an individual's information under certain conditions, such as in the case of information on pediatric cancer survivors. More information describing the impact of HIPAA on cancer registries may be found here: https://www.naaccr.org/data-security-confidentiality-issues/

Certificate of Confidentiality (CoC) – United States

"A Certificate of Confidentiality (CoC) is formal confidentiality protection authorized by the Public Health Service Act (PHSA) section 301 (d) (42 U.S.C § 241 (d)) to protect the privacy of human research participants enrolled in biomedical, behavioral, clinical and other forms of sensitive research by withholding identifying characteristics from those not connected to the research."[3] A CoC prohibits disclosure in response to legal demands, such as a subpoena. As of October 1, 2017, NIH-funded research activities are automatically issued a certificate under the NIH Policy on Certificates of Confidentiality. Although NAACCR does not receive personally identifiable information (PII) from registries, the use of deidentified Cancer in North America (CiNA) data or central registry data in research could include the risk that some combination of the information, a request for the information, and other available data sources could be used to deduce the identity of an individual, which is a case covered under the NIH CoC; the use of NAACCR CiNA data in research is an activity covered by the NIH CoC. More information on CoC is available here: https://humansubjects.nih.gov/coc/faqs#definitions and here: https://grants.nih.gov/policy/humansubjects/coc/information-protected-CoC.htm

[3] https://grants.nih.gov/policy/humansubjects/coc/what-is.htm

Assurance of Confidentiality (AoC) – United States

"An Assurance of Confidentiality [AOC] is a formal confidentiality protection authorized under Section 308(d) of the Public Health Service Act. It is used for projects conducted by CDC staff or contractors that involve the collection or maintenance of sensitive identifiable or potentially identifiable information. This protection allows CDC programs to assure individuals and institutions involved in research or non-research projects that those conducting the project will protect the confidentiality of the data collected."[4] Unlike the CoC, which applies to research, an AoC has broader applications to non-research projects and public health practice. More information on the AoC can be found here: https://www.cdc.gov/os/integrity/confidentiality/index.htm

Statistics Act – Canada

Data received by Statistics Canada is afforded the same level of security as any other data obtained under the authority of the Statistics Act. This Act also governs the return of records to the registries and transmission of microdata to other organizations, per standard Statistics Canada procedures for the protection of sensitive statistical information.
https://laws-lois.justice.gc.ca/eng/acts/s-19/fulltext.html

The Privacy Act/Loi sur la protection des renseignements personnels – Canada

"The Privacy Act is federal legislation that protects the personal information of Canadians in the hands of federal public sector institutions."
https://laws-lois.justice.gc.ca/pdf/P-21.pdf

Personal Information Protection and Electronic Documents Act (PIPEDA) – Canada

PIPEDA delineates rules for how private sector organizations involved in a commercial activity can collect, use, or share personal information, similar to the GDPR as described below.
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

[4] https://www.cdc.gov/os/integrity/confidentiality/index.htm

General Data Protection Regulation (GDPR) – European Economic Area

The GDPR is a European Union regulation regarding data protection and privacy, governing an array of data inclusive of individually identifiable health and/or medical information. Adopted in 2016, the protections of the GDPR apply to covered individuals, and requirements extend to organizations located anywhere in the world that "target, collect or process" data on these individuals whether the organizations processing and controlling these data are physically located within or beyond the European Economic Area (EEA). Cancer registries, depending on operational standards, may collect data subject to GDPR and, therefore might anticipate receipt of requests for patient-level data to which the obligations of GDPR compliance attach. Because NAACCR registries only collect data on patients when they are residents of and physically located in the United States or Canada, and not when they are physically located in the EEA, few if any data subject to the GDPR are likely to be curated in NAACCR registries. The context is additionally shaped by provisions of the GDPR that permit use of personal information on the basis of necessity in the area of public health – using a term and concept similarly introduced in recent revisions to the Common Rule.

A registry in receipt of a data request associated with GDPR compliance requirements may wish to provide the requestor with data only on the basis of advice and counsel from the registry's organization. With the many changes occurring in cancer surveillance, this document may not cover all instances where the GDPR could apply. Please consult the state law and regulations regarding PHI to individuals who are the EEA residents or physically residing in the EEA.

Additional resources describing the GDPR may be found here:
Johns Hopkins University GDPR Guidance: https://jhura.jhu.edu/compliance/gdpr/
Complete guide to GDPR compliance: https://gdpr.eu/

Appendix A – Request for Personal Health Information Template

REQUEST
For Personal Health Information

Cancer Registry Name
Cancer Registry Address

You have requested access to personal health information that is held by [Name of Cancer Registry]. There are some exceptions, but [Name of Cancer Registry] will accommodate all reasonable requests. This form allows you to request specific personal health information pertaining to you or someone that you have legal authority to request data on.

Patient Name: _____ Patient DOB:_____
Case Number or Social Security Number: _____
I authorize the [Cancer Registry Name] to release the following personal health information as requested and specified below:

☐ All information

☐ Information from a specific time period (specify dates):
From: _____ To: _____

☐ Information on a specific cancer:
Specific cancer type: _____

Mechanism of data delivery (please select one):

☐ Secure Email or other electronic method.

If email, please print email address: _____

☐ U.S. Mail. If U.S. mail, please print address where you would like to receive requested information:

Address: _____

City, State, ZIP: _____

Phone Number: _____

Signature of requestor: _____ Date: _____

Printed name of requestor: _____

Relationship to patient: _____

Please include documents verifying your identity and, if applicable, relationship to patient.