



North American Association of Central Cancer Registries

2002 NAACCR Workshop Report:

North of the Border Workshop I: Surveillance Data Access and Confidentiality Protection in Canadian Cancer Registries



April 3–4, 2002

Banff Park Lodge
Banff, Alberta, Canada

Suggested Citation:

NAACCR. 2002 NAACCR Workshop Report: North of the Border Workshop I: Surveillance Data Access and Confidentiality Protection in Canadian Cancer Registries. Springfield (IL): North American Association of Central Cancer Registries, July 2002. 41 pp.

Table of Contents

Executive Summary	iv
Participants List	viii
Welcome and Introduction.....	1
Data Use and Confidentiality in Canadian Cancer Registries: The Delicate Balance	2
Defining Best Practices.....	4
Application of Privacy Principles to Access and Use of Registry Data for Surveillance and Research	4
Consent for the Collection, Use, and Disclosure of Registry Data.....	6
Variation in NAACCR Member Policies for Patient Contact in Epidemiological Studies	8
Statistics Canada Legislative and Policy Framework.....	10
Access and Confidentiality: Health Canada’s Perspective	11
Overview of Technical Issues in Protection of Confidentiality.....	13
The Road To Use of Multi-Registry Aggregated Data Files	15
Data Confidentiality and the NCI SEER Program.....	17
Manitoba Linked Databases: Access, Use, and Dissemination	20
Access and Use Policies: UBC Linked Health Data Project	21
Breakout Group Reports	22
Next Steps/Closing Remarks	27
Action Items.....	28
Appendix A: The 10 Privacy Commandments	28
Appendix B: Privacy Policy/Code for a Canadian Cancer Registry.....	30
Appendix C: Factors To Consider in Determining When It Is Impracticable To Obtain Consent	39
Appendix D: Web Addresses for Organizations and Documents Discussed at the North of the Border Workshop	40

**North American Association of Central Cancer Registries
2002 NAACCR Workshop Report: North of the Border Workshop I:
Surveillance Data Access and Confidentiality Protection
in Canadian Cancer Registries**

**April 3–4, 2002
Banff Park Lodge
Banff, Alberta, Canada**

Executive Summary

Mary McBride, Director of the British Columbia Cancer Registry and Chair of the Workshop Planning Committee, welcomed participants to the North of the Border Workshop. She explained the workshop goals and objectives (i.e., to develop a plan to adopt and adapt privacy guidelines for cancer registries), and provided definitions of the terms “privacy,” “confidentiality,” and “security.” Mr. David Gouthro, workshop Facilitator, provided participants with the following list of overriding questions to consider throughout the workshop: (1) Who has access to the information? (2) To what data do they have access? (3) For what purposes can the data be used? (4) Under what conditions can the data be used? (5) In addition to the primary use, are there other parties to whom the information can be distributed? (6) What conditions or requirements should be met before disseminating the results?

Eric Holowaty, Director of the Cancer Control Unit of Cancer Care Ontario, presented on data use and confidentiality in Canadian cancer registries and explained that cancer registries face increasing pressure to be more accountable to the public, have access to better information, and track the effectiveness and efficiency of their programs faster. Dr. Holowaty described how the core values and duties of cancer registries are framed within the Principles of Fair Information Practice, and suggested that there needs to be wider acceptance of these Principles. Such a move will require development of model policies and procedures related to confidentiality and the use and disclosure of sensitive information collected by registries, with the overall goal of developing best practices for collecting sensitive information.

Rachel Jean-Baptiste, Director of Science for the North American Association of Central Cancer Registries (NAACCR), provided definitions of the term “best practices,” including: (1) “a superior method or innovative approach that also consistently exceeds the standard level of performance based on expert review, evidence of significant improvement, and agreement of multiple sources;” and (2) “the most efficient way to perform a task.” Dr. Jean-Baptiste explained the differences between best practices for clinical application and best practices for organizational policies, noting that a process is not a best practice until it has been adapted to fit the environment of the adopting organization. She referred participants to the National Guideline Clearinghouse’s Web Site, www.guidelines.gov, for examples of best practice guidelines.

David Flaherty, a Canadian privacy consultant who specializes in health privacy issues, discussed the application of privacy principles to the access and use of cancer registry data for surveillance and research. Mr. Flaherty described current privacy laws in Canada and presented the 10 Privacy Commandments. One significant challenge is that the national privacy laws in Canada are not coherent. Mr. Flaherty presented the most recent version of the Canadian Institute for Health Information's (CIHI) privacy policy, "Principles and Policies for the Protection of Personal Health Information and CIHI." He also distributed a template for cancer registries to use in developing their own privacy policies, which should be self regulatory, reflective of the registry's needs and goals, and should take privacy issues very seriously. Cancer registries should have a privacy officer, privacy team, and privacy policy in place. He noted that a current registry employee could take on the role of privacy officer (i.e., it is not a full-time job). It was suggested that a committee be formed to review Mr. Flaherty's template, modify and adapt the document for cancer registry use, and recommend next steps.

Patricia Kosseim, Senior Ethics Policy Advisor at the Canadian Institutes of Health Research (CIHR) discussed issues of consent for the collection, use, and disclosure of cancer registry data. Bridging the knowledge and language gaps between the research community and consumers, policymakers, and private organizations has been a goal of CIHR. Ms. Kosseim described efforts to articulate CIHR recommendations for the application of the Personal Information Protection of Electronic Documents Act in the health research area. She referred participants to the CIHR Web Site, www.cihr.ca, for these and other recommendations. Ms. Kosseim also presented a proposed consent model in the form of a flow chart. She recommended that registries make every effort to gain public confidence and trust to maximize patients' willingness to consent and minimize their objections to the work conducted by cancer registries.

Carole Herbert, Senior Research Officer in the Cancer Surveillance Unit at Cancer Care Ontario reported on the results of a project to determine how cancer registries handle research applications that ask for specific identifying information for the purpose of contacting patients. She stated that these types of studies must be balanced with increasing privacy concerns and new legislation. It is hoped that this balance can be achieved via development of best practices. Dr. Holowaty then described results of a three-question survey that asked Ontario residents about their perceptions of invasion of privacy. He concluded that cancer registries should not take public support for granted, and that if registries effectively describe the use of their information systems, who the users are, and what security measures are taken, the general public's perception of registries and their work will become more positive.

Gary Catlin, Director of the Health Statistics Division at Statistics Canada, discussed the mandate, legislative policy framework, and role of Statistics Canada. Mr. Catlin also described the Statistics Act and emphasized Statistics Canada's responsibility and commitment to protecting confidentiality by ensuring that: (1) everyone who works at Statistics Canada takes an oath of office to protect the confidentiality of the data; and (2) if data are released, the responsible individuals can be prosecuted. He explained Statistics Canada's record linkage policy and referred participants to the Statistics Canada Web Site, www.statcan.ca. Mr. Catlin also noted that Statistics Canada has a companion guide to the Statistics Act that explains the 10 Privacy Commandments and is geared toward a lay audience.

Barbara Foster, who is in the Cancer Bureau at Health Canada, explained that the organization's mission is to improve and maintain the health of all Canadians. She presented Health Canada's approach to privacy issues. Ms. Foster highlighted four examples: (1) Statistics Canada and the Surveillance Risk Assessment Division, (2) the Childhood Cancer Surveillance and Control Program, (3) the National Enhanced Cancer Surveillance System, and (4) the Canadian Breast Cancer Screening Database. Ms. Foster noted that Health Canada is at a crossroads in that it needs to determine, within a cancer control framework, whether to address research and surveillance together or separately. She stated that provinces, Statistics Canada, and Health Canada need to work together more effectively, and added that the results of this workshop will be useful to the newly formed Canadian Cancer Surveillance Alliance.

Gerry Bliss, Chair of the IT Committee at the Canadian Organization for the Advancement of Computers in Health (COACH) provided an overview of technical issues in the protection of confidentiality and examples of how cancer registries can protect confidentiality from an IT perspective. Mr. Bliss described a document titled "COACH Guidelines for the Protection of Confidential Information," which addresses privacy issues and has been recommended for use by organizations attempting to comply with current security standards. He noted that even the best security tools will fail if an organization does not have a culture that understands the value of privacy and practices secure behavior. Cancer registries may be able to partner with other organizations to share resources, and it is critical that the information technology staff and privacy staff at registries work closely together.

Holly L. Howe, NAACCR's Executive Director, described the development of multi-registry aggregated data files at NAACCR, focusing on Cancer in North America (CINA) Deluxe and CINA+ Online. CINA+ Online, NAACCR's only public use data file, has been released. Dr. Howe also described results of beta testing CINA Deluxe and the current and potential future uses of CINA Deluxe and CINA+ Online. To alleviate registry concerns regarding confidentiality, NAACCR Assurances and Researcher Agreements were developed and are available on the NAACCR Web Site at www.naacr.org. Dr. Howe also discussed lessons learned from the first CINA Deluxe Beta test (NAACCR currently is moving into the second round of testing).

Lynn Ries, a Health Statistician in the Surveillance, Epidemiology and End Results (SEER) Program at the National Cancer Institute, discussed aspects of data confidentiality as they relate to the SEER Program. Ms. Ries described the SEER Program's public use agreement, which was based on the National Center for Health Statistics' public use agreement. She explained that SEER is trying to balance patient confidentiality concerns with maximal analysis of the data.

Erich Kliewer, Director of Cancer-Care Manitoba's Department of Preventive Oncology and Epidemiology, described access, use, and dissemination of Manitoba linked databases. He explained that the reporting of cancer cases in Manitoba is legally mandated through the Public Health Act and its associated regulations. Dr. Kliewer described data use policies at three institutions that can perform data linkage: (1) Cancer-Care Manitoba, (2) Manitoba Health, and (3) the Manitoba Centre for Health Policy at the University of Manitoba. One particular challenge is that Cancer-Care Manitoba and Manitoba Health do not have a clearly written formal policy that outlines the steps individuals must take to access the data.

Ms. McBride presented on access and use policies related to the University of British Columbia's (UBC) Linked Health Data Project. She described access to the data, and referred participants to the following Web site: www.chspr.ubc.ca, for more information on access policies related to the UBC linked health database.

Participants were assigned to one of the following four breakout groups defined according to types of registry data access with different levels of sensitivity to confidentiality issues:

- “Aggregate or statistical data (i.e., no person-specific information is released).”
- “Person-specific information is included in the data provided to the requestor, but all individual identifiers are removed. Includes public use files.”
- “Person-specific information and identifiers are included in the data provided to the requestor, but no contact with individuals will occur, and individuals are not expected to be directly affected in any way by the research. Includes record linkage studies.” And: “Person-specific information and personal identifiers are included in the information provided to the requestor, and there is a possibility or likelihood that the information will indirectly affect future patient management for those individuals, although individuals will not be contacted directly. Includes record linkage studies.”
- “Person-specific information and personal identifiers are included in the data provided to the requestor, who intends to use the information to contact subjects or their families. The purpose of any contact and followup would (not?) necessarily be considered research.”

Each breakout group addressed the following question in trying to develop a common set of recommendations and best practices for their respective types of data sets: “What guidelines do you recommend regarding the release of this category of data?”

Ms. McBride closed the workshop by outlining next steps and thanking participants, consultants, sponsors, and the Workshop Planning Committee for their involvement. She identified the following action items:

- Circulate the report from this workshop to participants, receive participant feedback, and incorporate revisions into a revised report
- Develop a plan to adopt and adapt privacy guidelines for cancer registries
- Establish a committee to review Mr. Flaherty's General Privacy Policy that could be customized to fit the needs of cancer registries, modify and adapt that document for cancer registries, and recommend next steps.

Participants List

Michel Beaupre

Director
Quebec Cancer Registry
Service de la question des donnees
Fichier des Tumeurs du Quebec
1125 Chemin St. Louis
Sillery, Quebec G1S 1E7
CANADA
Phone: 418-266-6739
Fax: 418-643-5468
E-mail:
michel.beaupre@msss.gouv.qc.ca

Dr. Neil Berman

Strategic Partnerships Office
Cancer Division
Health Canada
PL 1901 A2
A920, Jeanne-Mance Building
Tunney's Pasture
Ottawa, Ontario K1A 1B4
CANADA
Phone: 613-954-1591
Fax: 613-941-0443
E-mail: neil_berman@hc-sc.gc.ca

Gerry Bliss*

Chair
IT Committee
Canadian Organization for the
Advancement of Computers in
Health
Phone: 403-241-7374
E-mail: gerry.bliss@shaw.ca

Gary Catlin*

Director
Health Statistics Division
Statistics Canada
18-F, R.H. Coats Building
Tunney's Pasture
Ottawa, Ontario K1A 0T6
CANADA
Phone: 613-951-8571
Fax: 613-951-0792
E-mail: gary.catlin@statcan.ca

Dr. Vivien Chen

Director/Epidemiologist
Louisiana Tumor Registry
Department of Public Health and
Preventive Medicine
Louisiana State University Health
Sciences Center
1600 Canal Street, Suite 900A
New Orleans, LA 70112
Phone: 504-568-4716
Fax: 504-568-2493
E-mail: vchen@lsuhsc.edu

Michel Cormier

Manager of Canadian Cancer
Registries
Health Statistics Division
Statistics Canada
18-O, R.H. Coats Building
Tunney's Pasture
Ottawa, Ontario K1A 0T6
CANADA
Phone: 613-951-1641
Fax: 613-951-0792
E-mail:
michel.cormier@statcan.ca

Darlene Dale+

Manager
Ontario Cancer Registry
Cancer Surveillance Unit
Cancer Care Ontario
620 University Avenue
Toronto, Ontario M5G 2L7
CANADA
E-mail:
darlene.dale@cancercare.on.ca

David Flaherty*

Privacy Consultant
1939 Mayfair Drive
Victoria, BC V8P 1R1
CANADA
Phone: 250-595-8897
Fax: 250-595-8884
E-mail: david@flaherty.com

Barbara Foster*

Cancer Bureau
Health Canada
First Floor, Room 1340
Building 6, AL 0601C1
Tunney's Pasture
Ottawa, Ontario K1A 0L2
CANADA
Phone: 613-952-2775
Fax: 613-941-2057
E-mail:
barbara_foster@hc-sc.gc.caDr.

David Gouthro

Facilitator
The Consulting Edge: Movers
& Shakers, Inc.
23-1551 Johnston Street
Vancouver, BC V6H 3R9
CANADA
Phone: 800-685-6818
E-mail:
dgouthro@theconsultingedge.com

Caroline Galvin

New Brunswick Department
of Health and Wellness
P.O. Box 5100
Carleton Place
520 King Street, Second Floor
Fredericton, New Brunswick
E3B 5G8
CANADA
Phone: 506-453-2536
Fax: 506-444-4697

Dr. Juanita Hatcher

Cross Cancer Institute
Fifth Floor
11560 University Avenue
Edmonton, Alberta T6G 1Z2
CANADA
Phone: 780-432-8650
E-mail:
juanitah@cancerboard.ab.ca

* = **Speaker**

+ = **Planning Committee Member**

Carole Herbert*+
Senior Research Officer
Cancer Surveillance Unit
Cancer Care Ontario
620 University Avenue
Toronto Ontario M5G 2L7
CANADA
Phone: 416-971-5100, ext. 2245
Fax: 416-971-6888
E-mail:
carole.herbert@cancercare.on.ca

Dr. Eric Holowaty*+
Director
Cancer Surveillance Unit
Cancer Care Ontario
620 University Avenue
Toronto, Ontario M5G 2L7
CANADA
E-mail:
eric.holowaty@cancercare.on.ca

Dr. Holly L. Howe*
Executive Director
NAACCR
Suite C
2121 W. White Oaks Drive
Springfield, IL 62704
Phone: 217-698-0800, ext. 2
Fax: 217-698-0188
E-mail: hhowe@naaccr.org

Dr. Rachel Jean-Baptiste*+
Director of Science
NAACCR
Suite C
2121 W. White Oaks Drive
Springfield, IL 62704
Phone: 217-698-0800, ext. 5
Fax: 217-698-0188
E-mail: rjeanbap@naaccr.org

Sarah Kettel
Health Canada
LCDC Building, Second Floor
Tunney's Pasture, AL 0601C1
Ottawa, Ontario K1A 9L2
CANADA
Phone: 613-954-4793
Fax: 613-941-5497
E-mail: sarah_kettel@hc-sc.gc.ca

Dr. Erich Kliewer*+
Director
Department of Preventive
Oncology and Epidemiology
Cancer-Care Manitoba
675 McDermot Street
Winnipeg, Manitoba R3E 0V9
CANADA
Phone: 204-787-2174
Fax: 204-783-6875
E-mail:
erich.kliewer@cancercare.mb.ca

Patricia Kosseim*
Senior Ethics Policy Advisor
Ethics Office
Canadian Institutes of Health
Research
410 Laurier Avenue, West
Ottawa, Ontario K1A 0W9
CANADA
E-mail: pkosseim@cihr.ca

Jeri Kostyra
Manager
Manitoba Cancer Registry
Department of Preventive
Oncology and Epidemiology
Cancer-Care Manitoba
675 McDermot Street
Winnipeg, Manitoba R3E 0V9
CANADA
Phone: 204-787-2157
Fax: 204-783-6875
E-mail:
jeri.kostyra@cancercare.mb.ca

Maureen MacIntyre
Manager
Nova Scotia Cancer Registry
Bethune Building, Room 569
1278 Tower Road
Halifax, Nova Scotia B3H 2Y9
CANADA
E-mail: ccmmi@qe2-hsc.ns.ca

Jack Mackinnon
Northwest Territories Cancer
Registry
Department of Health and Social
Services
P.O. Box 1320
Yellowknife, NT X1A 2L9
CANADA
Phone: 403-920-8946
Fax: 403-873-0442
E-mail:
jack_mackinnon@gov.nt.ca

Mary McBride*+
Epidemiologist
Cancer Control Research
British Columbia Cancer Registry
600 W. 10th Avenue
Vancouver, BC V5Z 4E6
CANADA
Phone: 604-877-6122
Fax: 604-877-1868
E-mail: mmcbride@bccancer.bc.ca

Josee Menard
Health Statistics Division
Statistics Canada
18-O, R.H. Coats Building
Tunney's Pasture
Ottawa, Ontario K1A 0T6
CANADA
Phone: 613-951-1641
Fax: 613-951-0792
E-mail: josee.menard@statcan.ca

Bertha Paulse
Chief Executive Officer
Newfoundland Cancer Treatment
and Research Foundation
Murphy Cancer Centre
Health Sciences Centre
300 Prince Phillip Drive
St. John's, Newfoundland
A1B 3V6
CANADA
Phone: 709-777-7592
Fax: 709-753-0927
E-mail: bpaulse@nctrf.nf.ca

* = Speaker
+ = Planning Committee Member

Lynn Ries*
Health Statistician
SEER Program
Division of Cancer Control and
Population Sciences
National Cancer Institute
National Institutes of Health
Executive Plaza North, Room 343
MSC 7350
6130 Executive Boulevard
Bethesda, MD 20892-7350
Phone: 301-496-8510
Fax: 301-496-9949
E-mail: lr44c@nih.gov

Dianne Robson
Associate Director
Epidemiology and Preventive
Oncology
Saskatchewan Cancer Foundation
Allan Blair Cancer Centre
4101 Dewdney Avenue
Regina, Saskatchewan S4T 7T1
CANADA
Phone: 306-766-2695
Fax: 306-766-2179
E-mail: drobson@scf.sk.ca

Ghislaine Villeneuve+
Chief
Vital and Cancer Statistics
Health Statistics Division
Statistics Canada
18-O, R.H. Coats Building
Tunney's Pasture
Ottawa, Ontario K1A 0T6
CANADA
Phone: 613-951-1641
Fax: 613-951-0792
E-mail: villghi@statcan.ca

* = **Speaker**

+ = **Planning Committee Member**

WORKSHOP SUMMARY

Welcome and Introduction

Mary McBride

Mary McBride, Director of the British Columbia Cancer Registry and Chair of the Workshop Planning Committee, welcomed participants and noted that the workshop was developed by both Canadian and American members of the North American Association of Central Cancer Registries (NAACCR). The workshop was endorsed by the Canadian Council of Cancer Registries (CCCR) and received funding support from NAACCR, the National Cancer Institute (NCI), Health Canada, and Statistics Canada, with additional support from Cancer Care Ontario.

Ms. McBride explained that the workshop's objectives were to:

- Inform participants regarding principles and goals of data dissemination for cancer registries
- Inform participants regarding current principles and guidelines regarding research ethics and privacy/confidentiality legislation in Canada
- Evaluate best practices and policies of outside groups relevant to access, use, and dissemination of health surveillance data (e.g., NAACCR, the Surveillance, Epidemiology, and End Results [SEER] Program; the University of British Columbia [UBC] and Manitoba Linked Health Databases for Health Policy Research) in relation to cancer registry best practices
- Recommend policies and processes for access and use of registry data for these purposes, at both the national and provincial/territorial level
- Develop a common data confidentiality protection protocol, vetted by a privacy expert, for communication to partners and users.

Ms. McBride noted that the workshop would: (1) inform and educate participants on international privacy principles—and the latest Canadian legislation based on those principles—under which Canadian cancer registries need to operate; and (2) result in recommendations for a consensus set of guidelines for access and use of Canadian registry data for surveillance purposes, at both the national and provincial/territorial level. Specifically, the workshop would focus on how the privacy principles affect the use of registry data for surveillance and research. Examples of these activities include statistical reports for cancer cluster investigation, record linkage studies, epidemiologic studies that involve recontact of patients, and public use data files. Ms. McBride expressed hope that workshop participants would reach consensus on a set of guidelines for registry activities that are consistent with the privacy principles. She concluded her opening remarks by providing definitions of the following terms, developed by the National Academy of Sciences in the United States:

- **Privacy:** An individual's desire to limit the disclosure of personal information.
- **Confidentiality:** A condition in which information is shared or released in a controlled manner. The workshop is intended to develop a set of policies or guidelines to codify the rules by which registries control the release of personal information in an effort to protect patient privacy while fulfilling the mandate of cancer registries.
- **Security:** A number of measures that organizations implement in an effort to protect information and information systems. This includes efforts to maintain confidentiality as well as to ensure the integrity and availability of information and the information systems used to access data.

Mr. David Gouthro, the workshop Facilitator, asked participants to consider the following questions and formulate recommendations based on them during the course of the workshop: (1) Who has access to the information? (2) To what data do they have access? (3) For what purposes can the data be used? (4) Under what conditions can the data be used? (5) In addition to the primary use, are there other parties to whom the information can be distributed? (6) What conditions or requirements should be met before disseminating the results?

PART I: SETTING THE STAGE

Data Use and Confidentiality in Canadian Cancer Registries: The Delicate Balance

Dr. Eric Holowaty

Eric Holowaty, Director of the Cancer Control Unit of Cancer Care Ontario, explained that there is increasing public pressure for programs such as cancer registries to be more accountable to the public, to have access to better information, and to track the effectiveness and efficiency of registry programs. In the last decade, there has been a renewed interest in cancer surveillance and the development of information systems to track the pertinent state of health, costs, and potential benefits. There also has been an explosion in the informatics field over the past decade; the potential of the Internet is now being realized, as is the increasing importance of communications, faster computers, and devices for storing large amounts of electronic data. With these technological innovations come additional security and privacy concerns, particularly for the safeguard of health-related information. The Principles of Fair Information Practice and newer privacy laws have been developed to address these security and privacy concerns.

The consequences of overly restrictive security include avoidable clinical errors, reduced future benefits from research, reduced public health interventions or a reduction in their effectiveness, less productivity/higher administrative costs, and an erosion in the confidence of the public health system. Dr. Holowaty defined cancer surveillance as the pursuit of knowledge about cancer control through scientific means and the improvement of the public's health through the effective application of that knowledge. Necessary uses of surveillance systems include monitoring the past and current burden of cancer on the population, projecting the future burden,

identifying populations at higher risk for cancer, determining the availability of effective intervention programs, assessing the use and effectiveness of diagnostic tests, influencing policy formulation, and supporting administrative functions.

Dr. Holowaty noted that there are core values, duties, and virtues associated with cancer surveillance. Cancer registries want to be seen as virtuous in how they conduct their affairs and embody traits of honesty, industry, passion, patience, justice, and humility. Cancer registries also hold duties or obligations to a broad constituency: society (including patients and their caregivers), participants in research, sponsors of research, employers, and professional colleagues. Within the framework of cancer registry core values, duties, and virtues are the Principles of Fair Information Practice, which are becoming the framework for privacy and confidentiality, not only in terms of information systems, but also wherever personal information is housed, electronic or not.

Dr. Holowaty described eight Principles of Fair Information Practice:

- Collection limitation (only collect what is needed to meet the primary purpose)
- Data quality (measuring and improving for acceptable levels the quality of the information, correcting data)
- Purpose specification (be clear about why sensitive information is being captured)
- Use limitation (restricting its use to its primary intended purpose)
- Security safeguards (personnel policies, database security, physical measures according to modern standards or expectations)
- Openness (or transparency, be open to all stakeholders what the means of collection, the uses and users, and conditions are for disclosure)
- Individual participation (autonomy, informed consent, wherever possible preparing the informed consent prior to collection)
- Accountability (to all of the stakeholders).

Challenges and opportunities in the field of cancer surveillance include: (1) expansion and integration of cancer surveillance activities, (2) coordination of health information policy and privacy safeguards, (3) openness and transparency, (4) harmonization of laws and practices, (5) informed consent, (6) identifying and non-identifying information, (7) personnel and management practices, and (8) oversight and accountability. In terms of next steps, Dr. Holowaty expressed hope that there would be further acceptance of the Principles of Fair Information Practice. Such a move may require some modification or better articulation, with examples appropriate for a cancer registry as well as developing model policies and procedures

related to confidentiality and the use and disclosure of sensitive information collected by registries. An overall goal would be the development of best practices for collecting sensitive information.

Defining Best Practices

Dr. Rachel Jean-Baptiste

Rachel Jean-Baptiste, NAACCR's Director of Science, cited one article that defined best practices as "a superior method or innovative approach that also consistently exceeds the standard level of performance based on: (1) expert review, (2) evidence of significant improvement, and (3) agreement of multiple sources." Another definition of best practices is "the most efficient way to perform a task," this is the generally accepted definition of the term. Best practices need to be developed for protecting patient confidentiality. Best practices from a medical perspective are based on clinical research; are evidence based; have high internal validity; and are repeatable with little, if any, need for modification.

Dr. Jean-Baptiste provided examples of best practices for breast cancer screening (women over the age of 40 should receive an annual mammography and conduct monthly breast self exams) and colorectal cancer screening (for low-risk individuals, fecal occult blood tests are advised; for high-risk individuals, colonoscopy is recommended). She referred participants to the National Guideline Clearinghouse's Web Site, www.guidelines.gov, which has many examples of best practices guidelines for these and other medical conditions.

When developing best practices for policies, the evidence needed to formulate the best practices comes from expert opinion. Issues to consider include the effectiveness of the application, the affected population, and the appropriateness of the best practices. Adaptability and flexibility also are important elements. The best practices must have both high internal validity as well as high external validity—for best practices to be adopted, they must be flexible and allow for improvement while maintaining their effectiveness. Dr. Jean-Baptiste closed her remarks by noting that a process is not a best practice until it has been adapted to fit the total environment of the adopting organization.

Application of Privacy Principles to Access and Use of Registry Data for Surveillance and Research

David Flaherty

David Flaherty, a Canadian privacy consultant specializing in health privacy issues, described some of his previous projects related to privacy issues with the British Columbia Cancer Registry, Cancer Care Ontario, and the Ontario Ministry of Health. In the last year, he conducted a general assessment of how Health Canada handles privacy issues, and is trying to persuade the organization to establish a privacy officer, a privacy team, and a privacy policy. He noted that privacy policies for cancer registries should be self regulatory, reflective of the registry's needs and goals, and should take privacy very seriously.

Protecting the best interests of cancer registries is a difficult issue. The national law in Canada is not very coherent. Provinces such as Alberta, Quebec, and Manitoba have a great deal of privacy law, but none of it was drafted with the interests of cancer registries or researchers in mind. Mr. Flaherty, who also is the Chief Privacy Officer for the Canadian Institute for Health Information (CIHI), presented the latest version of CIHI's privacy policy, a document called "Principles and Policies for the Protection of Personal Health Information and CIHI." The policy was approved by CIHI's Board of Directors, and illustrates each policy with specific procedures. He noted that Canada's national privacy standard, the Personal Information Protection of Electronic Documents Act (PIPEDA), will apply to all uses of personal information in the private sector by January 1, 2004, unless individual provinces pass their own legislation.

Mr. Flaherty presented the 10 Privacy Commandments (see Appendix A). The Commandments flow logically from one to the next, and have been informally adopted as the national privacy standard in Canada. Mr. Flaherty has developed a document customized for cancer registry application of the 10 Privacy Commandments. His document is a checklist, and includes having a privacy officer and a privacy team. Mr. Flaherty emphasized that confidentiality is the lifeblood of organizations such as cancer registries and CIHI. Mr. Flaherty has developed and conducted privacy impact assessments for the Canadian Organ Replacement Registry, the Ontario Trauma Registry, and the Electronic Health Record Initiative of Hong Kong Hospital Authority. These privacy impact assessments have been so effective that the Treasury Board in Ottawa has determined that no new systems can be built without first conducting a privacy impact assessment.

Many privacy advocates are suspicious of researchers, Research Ethics Boards (REBs), cancer registries, and some federal agencies, in part because they do not understand the work or operation of these individuals and organizations, and do not feel properly consulted on their activities. Overzealous privacy advocates can be silenced by demonstrating the ongoing viability of the legitimate activities that are in the public interest. It is well recognized and publicly accepted that cancer registries should be mandatory. He recommended that cancer registries develop privacy policies customized to their province's legislation, and presented a general privacy policy that could be customized by cancer registries in this way (see Appendix B).

Mr. Flaherty discussed the consent clause found in the 10 Privacy Commandments. A fundamentalist position on privacy is that informed consent is needed for every use of personal information—a difficult task for secondary collectors of personal information. One way around this for secondary information collectors is to encourage the primary collector (e.g., hospital, doctor, or laboratory) to inform patients. Informing at that level is more a question of notice than of obtaining consent, he noted.

Discussion

When asked how to operationalize his recommendations in cancer registries that often are small organizations with limited resources, Mr. Flaherty explained that an existing registry staff member could take on the role of privacy officer, which does not need to be a full-time job. For developing and managing privacy policies, registries can look to CIHI as a resource. Cancer registries are very privacy intensive, meaning they collect a lot of personal information.

Registries should market their concerns for privacy to the public. Cancer research is extremely important for the residents of Canada, and it needs to occur through controlled conditions that protect confidentiality and privacy.

Consent for the Collection, Use, and Disclosure of Registry Data

Patricia Kosseim

Patricia Kosseim, Senior Ethics Policy Advisor in the Ethics Office at the Canadian Institutes of Health Research (CIHR), presented practical principles for the collection, use, and disclosure of registry data as well as a proposed consent model. Her discussion focused on the results of 3 years of work that started with a literature review of all relevant Canadian legislation respecting the protection of personal information in the area of health research. Results of the review were published to facilitate a comparative analysis of federal, provincial, and territorial laws in the public and private sectors. An international literature review canvassing approaches taken in other jurisdictions around the world also was conducted and has been published recently.

Ms. Kosseim described the results of a June 2000 CIHR workshop held to discuss emerging issues around the use, collection, and disclosure of personal information in the area of research. A major issue identified was the knowledge and language gaps between the research community and consumers, policymakers, and privacy advocates. One of the major recommendations from this workshop was for CIHR to facilitate dialog between stakeholders with a view to bridging these gaps. The CIHR attempted this via two parallel efforts. One effort was publishing a series of questions and answers about the Personal Information Protection and Electronic Documents Act (PIPEDA) for health researchers—an effort to bring the law home to researchers and describe how the law applies to them in their day-to-day work. The other effort involved presenting the researchers' stories to policymakers, privacy advocates, and the general public in a draft document that includes actual case studies involving the secondary use of data in research (this document is being prepared for final publication).

In June 2001, a consultation session of experts was held to discuss CIHR's draft recommendations for the interpretation and application of PIPEDA in the health research context. Subsequent to further consultations, indepth research, and analysis, these draft recommendations were finalized into a document, entitled "CIHR Recommendations on the Interpretation and Application of PIPEDA," released in November 2001. It is hoped that these recommendations will help inform and shape a harmonized legal framework that eventually will govern research activity in this country. Ms. Kosseim noted that these recommendations and many other resources are available on the CIHR Web Site, www.cihr.ca (the specific URL is: www.cihr-irsc.gc.ca/about_cihr/organization/ethics/initiatives_e.shtml).

Ms. Kosseim presented a proposed consent model in the form of a flow chart indicating three stages:

- **At the point of confirmed diagnosis or other trigger.** The model proposed that there be some general notification (e.g., poster, brochure, pamphlet) at the source of collection indicating that personal information will be transferred to the registry as well as an

explanation of the mandate and intended use of that information for surveillance and future use purposes, along with contact information (e.g., telephone number, Web site). In jurisdictions where there are voluntary or mandatory reporting schemes with protection from liability, consent would not be required. Where there is no voluntary or mandatory reporting scheme and no protection from liability, either express consent would be required or, at a minimum, an opt-out provision is needed.

- **At the time of disclosure/use for research.** This is the stage where personal information would be disclosed by a registry to a researcher, or used by the registry itself to conduct internal research. If data are truly non-identifiable, consent would not be required; however, there still remains a concern for potential group harm that should be considered. According to CIHR's Recommendations, non-identifiable data include:
 - Anonymized information that has been permanently stripped of all identifiers or aggregate information that has been grouped and averaged, such that the information has no reasonable potential for any organization to identify a specific individual
 - Unlinked information that, to the actual knowledge of the disclosing organization, the receiving organization cannot link with other accessible information by any reasonably foreseeable method, to identify a specific individual.

For secondary use or primary collection of identifiable data, consent should, as a rule, always be obtained. However, there may be situations where it is impracticable to obtain consent. CIHR's Recommendations propose a list of factors to consider when determining whether or not it is impracticable to obtain consent (see Appendix C). In such cases, consent would not be required, provided all other legal and ethical conditions are met.

In other situations where it is practicable to obtain consent, the registry should contact the individuals first to obtain permission prior to disclosing any identifying information to researchers. Where permission is given, the researcher then could contact the individual to more fully explain the research and seek informed consent to participate in the study. The model proposes that risk of harm be considered in determining the appropriate form of consent. If the risk of harm is less than minimal, the form of consent should be an opt-out procedure; whereas if the risk of harm is greater than minimal, then the express consent with an option to withdraw should be employed.

- **At all times.** At all times, it is the responsibility of the registry to be open and transparent about their activities by making available the following:
 - Description of the registry's mandate and authority
 - Purposes for which it collects personal information
 - Type of personal information collected and general account of its use

- Registry’s information management practices (e.g., access policies, security safeguards, retention/destruction guidelines, etc.)
- Contact details for an individual in the organization to whom inquiries can be made
- Complaint procedures and the right of redress for individuals
- Public record of uses and disclosures made for research purposes
- Description of research projects that accessed/used registry data
- Potential/actual social benefits
- Oversight and approvals obtained
- Reference to research results.

Ms. Kosseim concluded her remarks by stating that it is crucial to gain public confidence and trust to maximize patients’ willingness to consent, when asked, and to minimize their objections to the work conducted by cancer registries.

Variation in NAACCR Member Policies for Patient Contact in Epidemiological Studies

Carole Herbert

Dr. Eric Holowaty

Carole Herbert, Senior Research Officer in the Cancer Surveillance Unit at Cancer Care Ontario, presented the results of a project in which cancer registries were contacted to determine how they handle research applications that ask for specific identifying information for the purpose of contacting patients. She noted that cancer registries are one of the only ways to obtain information that is specific to individual patients with a specific cancer. Ms. Herbert noted that when researchers apply to the Ontario Cancer Registry for information at any level except for the aggregate level, their studies must have been peer reviewed; have REB/Institutional Review Board (IRB) approval; and a determination is made as to whether the research question can only be addressed if the identifying information is disclosed, whether the researcher has adequate security measures in place at their organization, and whether they have adequate resources to carry out the research.

Ms. Herbert and colleagues contacted 77 NAACCR registries by e-mail and asked the following questions: (1) if they are or ever have been used for patient contact studies; (2) if so, the volume of these studies over the past few years; (3) whether their registry had health department involvement; (4) whether or not they approach the physician for permission to give out the patient’s name and address; (5) whether that physician’s permission is active or passive; and (6) who makes the first contact with the patient. To date, there have been 33 responses: 10 from Canada and 23 from the United States. Every registry that replied indicated they did use their

information in this manner, although 5 registries indicated only minimal use. The range of studies was 2–25 per year, with a mean of 10. Ms. Herbert reported that 23 of the registries indicated department of health involvement, and all of the registries require an equivalent review process after peer-review and REB/IRB approval. A total of 13 registries indicated using active physician permission, and 16 used passive physician permission. For the first patient contact, 7 registries indicated using registry staff and 20 reported using the actual study staff.

Ms. Herbert ended her discussion by stating that these types of studies must be balanced with increasing privacy concerns and reality in new legislation. It is hoped that best practices can be developed to help achieve this balance.

Dr. Holowaty described preliminary results from a health monitoring survey comprised of three questions to assess how privacy invasion is perceived. This survey has been nested within a larger national Canadian health survey containing approximately 125 questions that is administered by telephone using random-digit dialing. The three-question add-on survey is being administered to a random sample of 750 Ontario residents. Dr. Holowaty explained that medical research generally has a positive image in Canada—particularly cancer research—however, surveys are indicating fairly consistently that there are some concerns about access to medical records. It was hypothesized that when the cancer research or screening purpose is clearly explained, non-consensual uses of personal information may be more compelling obligations for the general public than protecting and sustaining their privacy. Nevertheless, researchers and cancer registry operators should not take public support for granted.

Provisional response rates to the three-question survey are at approximately 85 percent. The following three questions were asked:

- **Question 1.** If the health department sent you a letter reminding you to have a cancer screening test, do you think this would be an invasion of your privacy?
- **Question 2.** If you had cancer, do you think it would be an invasion of your privacy if your provincial cancer agency looked up your old addresses for research (e.g., studies to determine whether cancer incidence is related to living around polluted areas)?
- **Question 3.** If you had cancer and a legitimate research group wanted to study the risk of cancer from substances where you used to work, if the provincial cancer registry gave your name and address to these cancer researchers on a confidential basis so they could ask you if you wanted to take part in their research, do you think this would be an invasion of your privacy?

Survey participants who responded that any/all of the above scenarios constituted an invasion of their privacy also were asked if the perceived invasion of privacy would be justified or acceptable to them.

Provisional results based on about 600 replies indicate that for the first two scenarios, between 80 and 85 percent of participants felt that it was not an invasion of privacy. About two-thirds of the 15–20 percent who felt that it was an invasion also felt that it was justified. Dr. Holowaty

reported that there was slightly less support for the third scenario (the most intrusive) than for the first two. Only 2 participants disapproved of all three scenarios. He concluded his presentation by stating that the more effectively organizations describe the use of their information systems, who the users are, and what security measures are taken, the more positive the views of the general public.

Statistics Canada Legislative and Policy Framework

Gary Catlin

Gary Catlin, Director of the Health Statistics Division at Statistics Canada, discussed the legal mandate of Statistics Canada and its powers and responsibilities. The law that establishes Statistics Canada—the Statistics Act—is powerful. It gives the agency the authority and power to collect, compile, analyze, abstract, and publish information on economic, social, and general conditions of the country and its citizens. The broad range of information includes topics such as health and welfare, health services, education, retail, and business. In addition, Statistics Canada plays a leadership and coordination role for other organizations (e.g., cancer registries). Part of this role includes: (1) collaborating with other government departments for the collection, compilation, and publication of statistics (so there are standards used for the collection of information and sharing information); (2) promoting the avoidance of duplication of information collected; (3) promoting and developing integrated social and economic statistics dealing with all of Canada and each of the provinces; and (4) promoting the use of the collected data.

Mr. Catlin emphasized that Statistics Canada has a responsibility and a commitment to protect confidentiality. Two provisions of the Statistics Act underline the core confidentiality character of this commitment: (1) everyone who works within Statistics Canada takes an oath of office to protect the confidentiality of the information; and (2) if data are released, the individuals who are responsible can be prosecuted—there are provisions for fines and imprisonment for instances when individuals intentionally release information inappropriately.

When cancer registry data are released to Health Canada, the data are released down to the microdata level. Permission from all Canadian cancer registries has been granted for this type of release, but it is up to the Chief Statistician to sign an order to allow this release. The released information must only be for statistical and research purposes; data cannot be released for administrative purposes. Access to certain identifiable information may be provided when: (1) information is needed for statistical or analytical purposes, and (2) the information released does not disadvantage Statistics Canada's respondents and does not harm the relationship between the agency and its respondents.

Mr. Catlin explained that microdata files are individual, person-level files that are produced by surveys. Statistics Canada releases those files for public use when release substantially enhances the value of the data collected and only when it is satisfied that all reasonable steps have been taken to prevent identification on particular survey units. However, the agency is in discussion with its Microdata Release Committee to find ways of having a public use microdata file based on the cancer registry through screening or sampling from a file. Statistics Canada has yet to

release a microdata file from an administrative source like a cancer registry based on concerns that individuals could be identified.

Mr. Catlin described Statistics Canada's record linkage policy. Record linkage occurs for statistical and research purposes only, and the following must be demonstrated: (1) there is a cost-benefit advantage to the record linkage in that it has savings in terms of respondent burden; (2) there are benefits to be derived that are in the public interest; (3) there is a very thorough review of those proposals within Statistics Canada; and (4) the linkage is judged not to jeopardize the future conduct of Statistics Canada programs. In recent years, Statistics Canada has been posting record linkage proposals and the results of those proposals on their Web site, www.statcan.ca.

Statistics Canada has a privacy officer and a privacy team, and is starting to run privacy impact assessments. Only employees with a need-to-know can access sensitive statistical information. Of the 130 employees in the health statistics division, Mr. Catlin reported that only about 6 individuals ever have access to the cancer files, which are kept in a secure environment. Sensitive statistical information (i.e., confidential data) resides only on a secure network to which public access is not allowed (e.g., there is no Internet access on this network). There also are physical security measures taken for the transmission of sensitive information within Statistics Canada.

Discussion

In discussion, it was noted that once the data are collected, they fall under the auspices of the Statistics Act, meaning Statistics Canada cannot release them for administrative purposes, although they can release them for statistical and research purposes. Individuals who want access to the data must go to the provinces. There is a mandate within Statistics Canada to establish an REB to look at proposals for record linkages and surveys; this REB will include individuals outside of Statistics Canada who will offer advice to Statistics Canada's Record Linkage Committee. Statistics Canada has a companion guide to the Statistics Act that explains the 10 Privacy Commandments and is geared toward a lay audience.

Access and Confidentiality: Health Canada's Perspective

Barbara Foster

Barbara Foster, who is in the Cancer Bureau at Health Canada, described Health Canada's approach to privacy issues. Health Canada's mission is to improve and maintain the health of all Canadians. She provided four examples of databases and focused on access and use of information in these databases balanced with privacy and confidentiality security approaches.

- **Statistics Canada and the Surveillance and Risk Assessment Division.** Health Canada has a Memorandum of Understanding (MOU) with Statistics Canada. In that MOU, Health Canada is obtaining non-identifiable data for Canadian Cancer Statistics—a collaborative project between the provincial and territory registries, Statistics Canada, the National Cancer Institute of Canada, and Health Canada. The MOU also allows

Health Canada to conduct cancer surveillance online. There is a minimal cost, which is covered by Health Canada. The MOU is going to be expanded to allow Health Canada to obtain more variables so that survival analyses and other research can be conducted. Before Health Canada can link that data, it needs approval/permission/authorization from Statistics Canada and the provinces.

- **Childhood Cancer Surveillance and Control Program.** This program has an effective written consent policy, signed by the parent/guardian of the patient, that clearly outlines what is being done. Each of the 17 pediatric centers across Canada has all access and rights to the data, but the data are collated at Health Canada (i.e., Health Canada is the manager of the database, but not of the data). To use that data, a request must pass through a Program Management Committee, which is comprised of individuals from Health Canada, pediatric center representatives, representatives from outside organizations, and epidemiologists. The centers are notified of any use of the data, and are responsible for its quality. Only those employees who need to have access to that information are permitted to do so, and they must sign a confidentiality pledge. Requests for record linkages must be authorized by the Program Management Committee. The only data that are published are the aggregate data.
- **National Enhanced Cancer Surveillance System.** This is a collaborative effort of the provinces, territories, Health Canada, and Statistics Canada for a case-controlled study in which information is collected on cancer patients through a detailed questionnaire. Access to the data by outside groups is important for making optimal use of the data for broad and creative uses. A letter of intent must be submitted to a committee comprised of representatives from Health Canada, epidemiologists, and outside organizations. If the data are going to be used, the provincial investigators must be informed. The provinces have unlimited access and rights to that database, and they are responsible for physician consent issues. Health Canada manages the database. There is a confidentiality pledge that must be signed before use of the data, and only aggregate data are published.
- **Canadian Breast Cancer Screening Database.** In addition to the policies outlined for the National Enhanced Cancer Surveillance System, Health Canada has an individual MOU with each province that is submitting breast cancer screening information to Health Canada. Provinces have individual veto power.

Ms. Foster noted that Health Canada's relationship with CIHI is driven by CIHI on a case-by-case basis. Health Canada is beginning to work on privacy guidelines that take into account the 10 Privacy Commandments. She noted that although the Canadian cancer registries have been in existence for many years, Health Canada has only recently started working with them. Health Canada is at a crossroads—it needs to determine, in a cancer control framework, whether to address research and surveillance together or separately. Within the cancer arena, there are repositories of information (e.g., provinces, CIHI, etc.), and to plan for the future, allocate resources, and plan programs, these repositories of information must be linked. Provinces, Statistics Canada, and Health Canada all need to work more effectively together. Ms. Foster concluded her presentation by noting that the results of this workshop would be extremely useful for the newly formed Canadian Cancer Surveillance Alliance.

Overview of Technical Issues in Protection of Confidentiality

Gerry Bliss

Gerry Bliss, Chair of the IT Committee at the Canadian Organization for the Advancement of Computers in Health (COACH) opened his remarks by noting that the Gartner Group has predicted that safeguarding people, knowledge, systems, and nations will take priority for information technology (IT) resources in the coming years. He distributed an order form for the “COACH Guidelines for the Protection of Confidential Information,” a document that addresses privacy issues and has been recommended for use by organizations attempting to comply with current security standards.

Mr. Bliss stated that NAACCR is conducting some pioneering work in proactively establishing guidelines and standards for the intentional and strategic sharing of health information. As an organization, NAACCR represents more value in the information being shared than it being retained. Other organizations in the health system look to NAACCR for guidance in sharing health-related information, and the future of the health system depends on successful management of health information. Mr. Bliss discussed strategies for applying technology to issues around security and privacy, summarized the risks, and proposed a corporate strategy for organizations that are trying to address security and privacy.

Mr. Bliss noted that there are no technical solutions, only technical tools, and the best security tools will fail if an organization does not have a culture that understands the value of privacy and practices secure behavior. Ninety percent of privacy and security risk is attributable to human behavior; the other 10 percent of the risk is related to computer systems, based on what humans tell computers to do. It is possible to deliver IT security without delivering privacy security, but it is impossible to deliver privacy security without IT security. Because it is not practical to deliver 100 percent security (that would mean 0 percent access), organizations have to live with the problems associated with access to information.

The first strategy of applying security to technology is to protect the perimeter. Protect internal networks with firewalls to block ports, limit traffic, and flag unusual content or traffic. Mr. Bliss reminded participants that firewalls do not look for attacks; they only generate reports on what they log. Intrusion detection systems are the newest aspect of network protection and do look at patterns of network packet behavior and consistency among packets or groups of packets and start analyzing network traffic to decide if there is an attack. However, the problem with all of these tools and technological advances is that they need to be constantly updated. He advised participants to block and eliminate viruses and related codes, and to filter spam out and quarantine high-risk attachments. Once the network is secure, internal and external connections need to be considered. Eliminate permanently connected modems, which can lead to open holes in the firewall. Virtual private networks can be used to create an encrypted tunnel for transmitting information from outside into the network. All of the privacy protection installed around the organization’s primary network must extend into the remote access devices (e.g., home PCs, laptops, personal digital assistants). He recommended that registries enter agreements with employees and others who access the network remotely to ensure they have this level of protection.

The second strategy is to control access. Mr. Bliss advised securing all settings in hardware and software so that the default passwords are changed to real passwords, and all of the system commands are limited to the system administrator and his or her staff. Every day, new holes in servers, hardware, and software are found; and there has to be a plan in place to patch those holes and manage those alerts. Passwords should expire in 90 days, and there should be a standard whereby after three unsuccessful log on attempts, the system freezes. Passwords also should be alphanumeric with upper- and lower-case characters. Registries should document and limit who has administration access. Mr. Bliss also recommended that registries encrypt data in their databases, when they move it internally or across their network, and when it is put on disposable/transportable media. Disposable/transportable media should be labeled in such a way that only the sender and recipient know what that media contains. In addition, it is advisable to destroy decommissioned media and hardware rather than trying to refurbish them.

The third strategy is to observe activity. Mr. Bliss recommended that registries turn on logs, and house them in special servers that are extraordinarily well protected so that the logs cannot be altered. It is important to monitor network activity and look for failed access attempts. However, avoid monitoring individual activity unless recommended by an individual's manager that there have been instances of network abuse.

Mr. Bliss presented a proposed set of strategies for an organization that is trying to protect privacy and security:

- Identify the person responsible for corporate IT risk management and establish the scope of their accountability. This role can be joined with the job of the privacy officer and should be part of the registry's privacy team.
- Select security standards that support privacy legislation compliance.
- Build and communicate policy that informs organizational behavior.
- Ensure that the security policy is linked to the privacy policy. Educate staff, partners, and providers to raise their awareness, communicate policy, and above all, change their behavior (this will cover more than one-half of the potential security holes).
- Assess the impact of every system change on privacy.
- Integrate IT security with the privacy team, particularly staff involved with corporate risk management.
- Design agreements around security behavior for staff; have all staff sign confidentiality agreements. Establish MOUs and information-sharing agreements with partners that define roles and responsibilities around security and privacy, and make sure the system providers have signed confidentiality agreements and are prepared to be reviewed and audited.

- Assess the current state, design the strategy, set targets, and measure progress at least annually.
- Use external auditors to corroborate internal audit findings.

Discussion

In discussion, it was noted that the issue of cost is a significant challenge for small organizations with limited resources, such as cancer registries. These organizations may be able to partner with other organizations, possibly within the same institute, to share resources. It is critical that the IT security staff and the privacy staff at these organizations work closely together.

PART II: REVIEW OF MODELS OF PUBLIC/RESEARCH USE FILES OF CANCER REGISTRY DATA

The Road To Use of Multi-Registry Aggregated Data Files

Dr. Holly L. Howe

Holly L. Howe, Executive Director of NAACCR, described the generation of multi-registry aggregated data files, starting in 1994 at the NAACCR Annual Meeting, where it was recommended that more information be produced from the NAACCR Call for Data and the monograph titled “Cancer in North America” (CINA). At this time, the statistical computations for these efforts were contributed on a volunteer basis. A NAACCR meeting in Colorado Springs held in 1997 led to the publication of a report titled “Recommendations for Public Use Files of National Cancer Data.” The report recommended that NAACCR:

- Release multiple public use data files designed to address user needs and the kinds of questions researchers want to answer
- Produce four different public use files:
 - CINA Plus (CINA+) Online, which would be manipulatable and could be used to examine age-specific information
 - CINA Deluxe, which would include more information and more variables—the data would be more identifiable, so additional protection and processes would be necessary to access these data
 - Two analytical files at the individual record level: a general analytic file and a research analytic file.

- Produce a greater capacity to release text-based information other than evaluating information from the dataset
- Conduct a CINA Deluxe beta test.

CINA+ Online, NAACCR's only public use data file, has been released. NAACCR is in the process of producing CINA Deluxe, and has conducted a beta test that identified numerous issues. The beta test was designed to address issues of the utility of the data files, issues related to confidentiality, if the data could be breached, if identifiability was possible should the files become corrupt, and if the data had reliability and quality across the registries. NAACCR decided to produce two files that could be used for analytic purposes: CINA+ Online, and the research analytic file, which is now CINA Deluxe. NAACCR also is using data submitted to CINA for producing aggregated text-based information, presented in NAACCR's quarterly newsletter.

Dr. Howe described some of the successes and accomplishments of recent years. She reported that there has been tremendous volunteer commitment and expertise in developing useful and meaningful tools related to this work. NAACCR obtained support from NCI in the form of access to NCI's Statistical Analytic Unit, which now conducts all NAACCR statistical compilations, aggregations, and special studies—these are no longer volunteer-based activities. NAACCR also has obtained software support for CINA Deluxe—one criterion for this data file was that the data be embedded in a user-friendly software package—called SEER*Stat, developed by Information Management Services (IMS), Inc. Registry certification standards have been identified and adopted; NAACCR started certifying registries in 1997 and since that time, registries throughout the United States and Canada have improved tremendously and many now meet minimal quality standards for producing reliable, useful information. Since 1997, there has been a tremendous growth in the number of certified registries and in the recognized value of certification by an external organization. Beta testing in 1999 of the CINA Deluxe file required funding and support from organizations. Approximately 15 applications were reviewed and access was granted for studies that addressed either use, quality, or confidentiality. In 1999, Health Canada offered volunteer-contributed programming support for CINA+ Online.

However, registry concerns about confidentiality associated with these activities were enormous. Registries wanted to know how the data were being used. NAACCR subsequently developed NAACCR Assurances and Researcher Agreements to address these concerns. The NAACCR assurances and researcher agreements are available on the NAACCR Web Site at www.naacr.org (Web addresses for organizations and documents discussed at this workshop can be found in Appendix D). The NAACCR Assurance and Researcher Agreements have been accepted and used by NAACCR members. NAACCR has obtained agreement from all U.S. registries to use the data in NAACCR's analytic file. Data from CINA+ Online have been used by the American Cancer Society to determine cancer incidence rates starting in 2001 and to estimate new cancer cases. In the "Annual Report to the Nation on Cancer," data from CINA+ Online have been used to determine age-specific rates of cancer for 55 percent of the U.S. population.

Dr. Howe discussed lessons learned from the first CINA Deluxe Beta test. Currently, NAACCR is moving into the second round of testing. Dr. Howe described a project, completed as a CINA Deluxe Version 1 beta test to identify the percent of unique records in the data file. The data file was compared with the SEER Program public use file. It was found that the CINA dataset had a very low percentage of unique records, and the SEER file had a very high percentage of unique records. The Illinois State Cancer Registry has developed a system whereby any time it receives a data request, parameters for a public use data file are set so that no more than 5 percent of the records in the file are unique. For data researchers, parameters are set so the proportion of unique records is no more than 20 percent. The registry can produce a public use data file at the ZIP code level in which there are less than 2 percent unique records. Dr. Howe noted that this tool is under evaluation to make it more user-friendly so it might be made available to all registries. She concluded her remarks by describing how two NAACCR research groups are using CINA Deluxe for large studies of ovarian and breast cancer.

Data Confidentiality and the NCI SEER Program

Lynn Ries

Lynn Ries, a Health Statistician at NCI's SEER Program, explained that de-identified data are submitted twice per year to SEER (the data contain no names, addresses, Social Security numbers, etc.). In 1979–1980, data from 1973–1977 were published in Monograph 57, which was more than 1,000 pages long. A public use data file was created so that investigators could analyze data at lower levels, such as histology by 5-year age group. Ms. Ries noted that in the 1980s, there were no confidentiality agreements and very few public use files. The National Center for Health Statistics (NCHS) instituted a confidentiality statement beginning with mortality data in the late 1980s because of confidentiality concerns. SEER followed suit and patterned their confidentiality agreement after the one developed by NCHS.

NCHS provides the mortality data on all deaths in all U.S. states. They require separate data agreements depending on the level of geographic information needed by researchers. Ms. Ries presented the NCHS public use agreement, quoting one particular section: “NCHS does all it can to assure that the identity of data subjects cannot be disclosed, all direct identifiers, as well as characteristics that might lead to identifications, are omitted from the data set. Nevertheless, it may be possible in rare instances, through complex analysis and with outside information to ascertain from the data set the identity of particular persons or establishments. Considerable harm could ensue if this were done.”

Other parts of the agreement include the following statements:

- I will not use nor permit others to use the data in these sets in any way except for statistical reporting and analysis.
- I will not release nor permit others to release the data sets or any part of them to any person who is not a member of this organization, except with the approval of NCHS.

- I will not attempt to link nor permit others to attempt to link the data set with individually identifiable records from any other NCHS or non-NCHS data set.
- I will not attempt to use the data sets nor permit others to use them to learn the identity of any person or establishment included in any set.
- If I should inadvertently discover the identity of any person or establishment, then:
 - (1) I will make no use of this knowledge, and
 - (2) I will advise the Director of NCHS.

At the county level, the NCHS public use agreement specifies that no data on an identifiable case should be derivable through subtraction or other calculation from the combination of tables in a given publication. Furthermore, no data should permit disclosure when used in combination with other known data. Failure to comply with the NCHS public use agreement is punishable by law, with a fine of up to \$10,000 or up to 5 years in prison.

The SEER public use agreement is almost the same as that of the NCHS and reads: “It is of utmost importance to ensure the confidentiality of patients who have been diagnosed with cancer. Every effort has been made to exclude identifying information on individual patients from the computer files. Certain demographic information such as sex, race, etc. has been included for research purposes. It is mandatory that all research results be presented/published in a manner which ensures that no individual can be identified. In addition, there should be no attempt to identify individuals from any computer file nor to link with a computer file containing patient identifiers.”

Similar statements to those found in the NCHS agreement also appear:

- You will not use nor permit others to use the data in any way other than for statistical reporting and analysis.
- You will not present/publish data in which an individual can be identified.
- You will not attempt to link nor permit others to link the data with individually identified records in another database.
- You will not attempt to learn the identity of any person whose cancer data is contained in the supplied file(s).
- You will not release nor permit others to release the data in full or in part to any person except with the written approval of the SEER Program.

Ms. Ries explained that SEER is trying to balance concerns about patient confidentiality with maximal analysis of the data. This is being accomplished by: (1) making data electronically available at less detailed levels on the Web via publications such as FASTSTATS and CANQUES; (2) de-identifying the public use file further by removing month of birth, date of death, and census tract; and (3) using compressed binary format, which allows for the data to be processed through SEER*Stat yet very difficult to link to any other file.

Ms. Ries noted that most problems with confidentiality have been associated with special studies when questions have arisen as to how the investigator knew about a particular patient. In two instances, there were problems of investigators making data available on the Internet, but those individuals stopped as soon as they were questioned. There have been no problems with the identification of an individual from the public use file. She reported that there have been complaints from investigators who want Census tract information included for socioeconomic status analysis. She also explained that there may be concerns if a specific group were to be identified that might lead to embarrassment (e.g., high rates of liver cancer found in a particular group with implications of high alcohol consumption). Possible solutions to this problem include designing the file so that investigators can have only the information that they need and no more; or having several files but having patient ID numbers different on each so that they cannot be linked—this allows for the same patient to be linked within the same file to other records for multiple primary analysis.

Because the SEER office does not obtain identifiers, special agreements between the SEER areas and other government agencies take place to facilitate linkage studies (e.g. the Centers for Medicare and Medicaid Services [CMS]) and IRB approval. After the data are linked, all identifying information is removed. Ms. Ries described SEER-CMS linkage studies, noting that linkage studies for those 65 years and older have presented a wealth of information on cancer costs and cancer care. However, there are concerns not only about the confidentiality of the patient, but also of the physician and the facility from the CMS files. As an additional precaution, before papers are submitted to journals that are based on CMS studies, they are read by SEER Principal Investigators, CMS officials, and SEER to ensure that no person, facility, or physician can be identified by the analysis.

Ms. Ries concluded her presentation by identifying the following future directions:

- New technologies can provide encryption for certain variables.
- Data files can be created for specific uses, such as a file with specific details on some variables but removal of details for others.
- Determining ways to allow socioeconomic status-type analyses without the ability to identify census tract or county.
- Remove other variables from selected files such as birthplace and cause of death; or show them only at a higher level.
- More analysis of underlying populations to analyze the probability that a match of a record not known to have cancer is a real match (e.g., are there thousands in the population with the same race, sex, geographic area, or only a few? If it is known that a person has cancer, can you find their “record” in the database? How sure is the match? What additional information would the match give?).

Manitoba Linked Databases: Access, Use, and Dissemination

Dr. Erich Kliewer

Erich Kliewer, Director of the Department of Preventive Oncology and Epidemiology at Cancer-Care Manitoba, explained that the reporting of cancer cases in Manitoba is legally mandated through the Public Health Act and its associated regulations. This legislation mandates that all cancer cases have to be reported to the provincial government—Cancer-Care Manitoba is the designated institution in Manitoba, and the institution runs the registry on behalf of Manitoba Health. Cancer-Care Manitoba is a trustee of the data.

Dr. Kliewer quoted from the Cancer Treatment and Research Foundation Act, which states that “The objectives of the Foundation are the conduct... of research in cancer... adequate recording and compilation of cancer data...” It is a challenge for a cancer registry that is legally mandated to collect the data, work with the data, conduct research, and at the same time link the data with other organizations’ data, all while maintaining privacy and confidentiality.

Dr. Kliewer described three institutions at which it is possible to perform linkage of Manitoba cancer data:

- **Cancer-Care Manitoba.** Cancer-Care Manitoba has the capability to do the linkage, but typically does not do much linkage work.
- **Manitoba Health.** The majority of linkages are conducted at Manitoba Health, where the cancer registry is linked to various other data sets. The linkage of Manitoba Health data is facilitated by the fact that Dr. Kliewer is employed there. Additionally, several Cancer-Care Manitoba epidemiologists and programmer analysts have appointments at Manitoba Health, thereby improving access to the data.
- **Manitoba Centre for Health Policy.** The Manitoba Centre for Health Policy is housed within the University of Manitoba, and it has an old copy of the cancer registry incorporated into its databases. However, the Centre has not updated the database since 1996, and does not generally use the cancer data.

Dr. Kliewer noted that one particular challenge is that Cancer-Care Manitoba and Manitoba Health do not have a clearly written formal policy that outline the steps individuals must take to access the data. Work is underway at both institutions to address this issue. Dr. Kliewer described the path for access to data that must be taken from Cancer-Care Manitoba: (1) University of Manitoba’s Research Ethics Board, (2) Cancer Registry Access and Confidentiality Committee, (3) Cancer-Care Manitoba’s Resource Impact Committee, and (4) Agreement for Access To Personal Health Information for Research Purposes. He also outlined the path for access from Manitoba Health: (1) University of Manitoba’s Research Ethics Board, (2) Manitoba Health’s Health Information Privacy Committee, (3) Manitoba Health Research Agreement, and (4) Oath of Confidentiality.

Dr. Kliewer concluded his remarks by noting that the cancer registry is linkable to other databases, including population registry, hospital discharge, physician claims, pharmacy, communicable diseases, provincial laboratory, immunization, mental health, regional data, vital statistics, health surveys, perinatal, inflammatory bowel disease, and diabetes databases.

Access and Use Policies: UBC Linked Health Data Project

Mary McBride

Ms. McBride explained that the University of British Columbia (UBC) Linked Health Database is maintained at the UBC Centre for Health Services and Policy Research. The Centre maintains an extensive collection of linked data on British Columbia health care utilization, facilities, hospital discharge summaries, mental health, workers compensation, and the cancer registry. The objective of the Centre in maintaining these files is to facilitate the use of these data for research purposes.

Access policies for the UBC Linked Health Database are spelled out on the following Web site: www.chspr.ubc.ca (follow links to Health Information Development Unit). According to Ms. McBride, access policies were developed “to balance advanced research capabilities with the requirement to protect individual anonymity.” Each database maintained by the Centre has a designated data steward, and the Centre requires written authorization from this individual for each database to which access is required. UBC can assist applicants in identifying available relevant data, refining data access requests, and identifying the appropriate data steward(s) to whom requests for permission should be sent.

Ms. McBride described the following main points of the approval criteria: (1) ethical approval from UBC or another equivalent ethics committee (e.g., clinical or behavioral research board); (2) written description of request details; and (3) assurance that all reports or papers must be provided in advance to the data steward(s) for perusal in advance of publication (in some instances). The access request details are written requests for access and include:

- A statement on the necessity of the data and the linkage
- Information on the study objectives and purposes for which the data are being requested
- Details on the data requested
- Information on who will have access to the data
- The personal, physical, and database security arrangements where the data will be held and processed
- Assurances that no data on individual providers or patients will be released in public documents
- An indication that the data will be returned or destroyed upon completion of the project.

All data processing is undertaken on a cost recovery basis. The Ministry of Health maintains the linked data files, and the Health Information Development Unit (HIDU) prepares an estimate of the time and costs to determine resources and impact. Prospective users obtain written authorization from the data steward(s). In those situations involving more than simple extraction, the request is reviewed by the Centre's Data Resources Subcommittee. The prospective users are required to sign an "Agreement to Proceed With Data Preparation Form," which briefly outlines the project and the estimated costs, for which the user agrees to reimburse the Centre.

In terms of access to HIDU databases, Ms. McBride explained that all files maintained by the Centre are stored in a manner that physically restricts access. Only those individuals authorized to handle them actually do so. This includes a small number of Centre programming and research staff. Staff are required to file a "Solemn Declaration of Assurance of Confidentiality" with the Centre and with the data steward(s) who require such documentation. Data users must demonstrate that adequate confidentiality and security provisions are in place in their own facilities.

PART III: BREAKOUT GROUP REPORTS

Participants were assigned to one of four breakout groups according to level of sensitivity of data release and asked to consider what they heard in the presentations that is or may be related to the type of data set assigned to each breakout group. They also were asked to review a binder containing resources and background information. The four breakout groups were assigned as follows:

- **Group A:** "Aggregate or statistical data (i.e., no person-specific information is released)."
- **Group B:** "Person-specific information is included in the data provided to the requestor, but all individual identifiers are removed. Includes public use files."
- **Group C:** "Person-specific information and identifiers are included in the data provided to the requestor, but no contact with individuals will occur, and individuals are not expected to be directly affected in any way by the research. Includes record linkage studies." **And:** "Person-specific information and personal identifiers are included in the information provided to the requestor, and there is a possibility or likelihood that the information will indirectly affect future patient management for those individuals, although individuals will not be contacted directly. Includes record linkage studies."
- **Group E:** "Person-specific information and personal identifiers are included in the data provided to the requestor, who intends to use the information to contact subjects or their families. The purpose of any contact and followup would (not?) necessarily be considered research."

Rather than attempt to address each of the questions posed by Dr. Gouthro at the beginning of the workshop, it was decided that participants would try to answer this question: “What guidelines do you recommend regarding the release of this category of data?” Participants were reminded that their task was to develop a common set of recommendations and best practices—with the overall goal of creating a draft national guideline consistent with the privacy principles—that relate to the use of registry data for surveillance and research.

GROUP A

“Aggregate or statistical data (i.e., no person-specific information is released).”

Access should be allowed for all users conditional upon all other privacy principles being observed (e.g., security, transparency, etc.) A definition of statistical data (e.g., cross tabs; means, medians; rates [survival, incidence]; or ratios) is needed to determine what are reasonable data to release and to reduce the risk of exposure. Defining constraints is a major issue as well, and there needs to be more research in this area. Careful consideration must be given to what other information is inherent in the data being released.

Constraints are necessary to reduce the risk of disclosure to a reasonable minimum. If a population is small, approaches such as aggregating over years and reporting the annual average, the moving average, or the average over cancer sites could be used. Restraints should be based on denominators (populations). Rates and other measures are based on populations for stability and accuracy, and restraints should be used for all statistics, including counts (e.g., size of a population or person-years). One level of constraint for researchers would be planning or conducting REB-approved studies.

Additional questions to address include how to address: (1) the media, (2) populations of more than 100,000 (what is the U.S. guideline?), and (3) small populations that have a large incidence of cancer (e.g., population of 5,000 and an incidence of ≤ 0 or 40). More research is needed on these issues.

Random rounding should be used (e.g., standardizing, adding [-2, +2] at random to small amounts). Another issue that needs to be addressed is defining constraint for release (e.g., use of numerator and denominator, other information in statistics).

The community needs to be informed before public release of the data, and information should only be released after the community is informed of the statistics (e.g., provincial survival rates/information on special populations). Furthermore, the community, or at-risk/target population needs to be defined. It may be reasonable to release data to researchers without informing the community in certain circumstances. The data could be released to the Ministry of Health (as custodian of all the data), to researchers with a mid-level of constraint (depending on REB status), and to the media with a high level of constraint (i.e., populations have to be bigger). Reasons for release include Ministry of Health use (e.g., clusters, planning, surveillance, etc.); planning (e.g., researchers conducting REB-approved research); and media/public/commercial use (e.g., Web sites, monographs, publications).

Inherent in the release of any data should be an adequate interpretation or explanation of them that includes data quality indicators. Security of the data is required, as are different levels of constraint.

GROUP B

“Person-specific information is included in the data provided to the requestor, but all individual identifiers are removed. Includes public use files.”

This breakout group divided their recommendations into two areas: (1) public use files, and (2) *ad hoc* requests that do not include personal identifiers.

To create a public use microdata file consistent with the mandate of a cancer registry, the following steps must be taken: (1) define identifiable variables/U.S. Health Insurance Portability and Accountability Act (HIPAA) legislation; (2) decide on the types of uses for a public data file (e.g., which variables are needed to answer most of the questions); (3) ensure that each data file goes through a process of approval and risk assessment during development, and have a formal statement outlining this process; and (4) establish a process to assess the file for risk of personal identification (e.g., the Illinois State Cancer Registry’s program). Informed consent is not required for any use of this kind of public use data file.

Public use data files must be non-linkable and have a signed assurance agreement indicating that the user cannot sell, link, or produce a report that would potentially identify individuals. Every individual with access must sign this assurance agreement (no organizations can sign, all users must be identified). The files may be used only for reporting and analysis. Registries will have to ensure that an individual requestor cannot link to another file, and ensure due diligence, possibly conducting an impact assessment. Data file requestors also should sign an agreement with the following or similar wording: “By accepting this file, you agree to be audited should the ‘releaser’ of the data so decide.”

In terms of *ad hoc* requests that do not include personal identifiers, documentation and written requests are necessary. Registries should develop a standard form that specifies: the variables, the purpose/intent, and the requestor. To ensure minimal need to respond to this type of request, registries should consider whether the request can be met via a public use data file. Issues to consider: (1) Is it a case? (2) Is it a disclosure (outside user)? The British Columbia data request process could be used as a potential model for developing a standard form. It also was recommended that a standard CD-ROM application be developed.

It is crucial to ensure minimization of risk of personal identification. Registries should consult their registry advisory committee to determine what level of approval is needed for *ad hoc* requests. These requests should be subject to a stringent approval process (REB/registry advisory committee), and consideration should be given to variables that can be provided against risk of identification. The release form should specify that the data remain non-linkable, should

include an assurance agreement and expiration date, and should outline provisions for disposal of the file. The agreement must require the requestor to suppress small cells (to be defined when reporting), and to acknowledge the registry data in reports.

GROUP C/D

“Person-specific information and identifiers are included in the data provided to the requestor, but no contact with individuals will occur, and individuals are not expected to be directly affected in any way by the research. Includes record linkage studies.”

“Person-specific information and personal identifiers are included in the information provided to the requestor, and there is a possibility or likelihood that the information will indirectly affect future patient management for those individuals, although individuals will not be contacted directly. Includes record linkage studies.”

Reasons for disclosing the data in these situations include: (1) the study is in the public’s interest; (2) it is consistent with the registry’s purpose; (3) it is REB approved; (4) there is no other feasible way to answer the question of interest (e.g., a large proportion of individuals is likely to have relocated or died since the time the personal information originally was collected); and (5) individual consent is not feasible because of either potential bias or lack of continuing contact. Ongoing record linkages for cancer surveillance/public health studies (e.g., linking screening and registry databases for the promotion/evaluation of screening) require an appropriate level of approval and must operate under the same conditions of use.

Registries should advertise their purpose and data uses (transparency) to maintain and increase the public’s trust. There is value in activities that link registry data to other data and lead to cancer control information. These projects and their worth are highly recognized, as is the necessity for this level of disclosure for some of these activities.

Disclosing data in these situations must occur under controlled conditions to minimize the risk of losing confidentiality and security. Conditions for data release/disclosure in these situations include: (1) the data are only used for specific study, (2) a research agreement that outlines conditions of use (confidentiality) and who has access is signed by external users, and (3) the agency/researchers work in an environment with similar conditions of use—both agency and researcher responsible for protecting confidentiality and the security of the data. It should be specified in the research agreement that data handling and transfer needs conform to standard procedures to minimize the risk of disclosure. Registries may want to consider requiring a signed agreement from every person who will access the data (e.g., primary researcher, research assistants, students, and so on).

Registries will need to address issues related to chart access, including: (1) determining who has access (agency staff only or researcher as well?), (2) determining how access is tracked, (3) ensuring that there is no identifying (e.g., use study numbers), and (4) confidentiality

agreements. These types of requests will need to be approved by the registry's advisory/review committee to review the qualifications of researcher as well as the scientific and ethical validity of the project.

Linkage expertise (the quality of the linkage and the process and requirements for follow-back of unmatched cases) and linkage quality (the quality of the record linkage should be reported in publications and presentations) issues need to be considered. Poorly identified data do not link well.

Internal and external research should operate under the same conditions of use. Conditions of use include the following:

- A review of reports, results, and publications by the registry
- Ensuring there is no inadvertent disclosure
- Verifying interpretation
- Controlled destruction of data once purpose has been met
- Acknowledgement of the registry as the source of data
- Site audits (verification of agreement conditions)
- Linkage activity, as the most sensitive part of the process, conforms to high levels of security (e.g., only direct users have access, physical security)
- Linked data are anonymized unless there is an approved research use
- Agreement contains requirements to comply with current security standards
- Agreement contains a data flow, identifying where identifying data are held
- Requirement that researcher not relink linked data file back
- Identifiable data are defined
- Recognize that files with "identifiers have gradient of disclosure risk; researcher must justify disclosure of these as necessary"
- Pertains to record linkage, tissue and tumor procedures, and chart abstraction – conditions apply to all.

GROUP E

“Person-specific information and personal identifiers are included in the data provided to the requestor, who intends to use the information to contact subjects or their families. The purpose of any contact and followup would (not?) necessarily be considered research.”

In these situations, the feasibility of the study needs to be carefully determined, with special consideration given to privacy screening (e.g., are there “show stoppers,” or reasons to not even contemplate the study) and REB approval. Registries should conduct an internal review to assess protocol, REB submission and approval, privacy protection/risks, research contract, consent process, and response burden.

The contract, or confidentiality pledge, should be signed by registry staff, the principal investigator, and all colleagues who have access to identified data. The contract should include provisions for safeguards/storage of the data, return/destruction of the data, third party activities, the registry's right to audit and review publications, and the consent process.

Physician contact may occur when the patient knows their diagnosis, to determine patient wellness, to determine patient ability to participate, and to contact a surrogate. Patient contact (by the registry) may occur to assess content burden, number of times, and method. Written contact with interview questions and verifications is preferred.

The following questions need to be addressed: (1) Does using an M.D. as a "gatekeeper" deny patient autonomy? (2) Is the M.D. consent process active or passive? (3) How recently does the M.D. need to have seen the patient to determine the patient's current ability to participate? There should be an indicator to the registry of the patients desire for "contact" or "no contact."

Patient consent forms should include the following information (patients will not be identifiable in publications): (1) how much and what type of information is needed; (2) who can consent; (3) to whom the information is disclosed; (4) what specific information will be collected; and (5) permission to contact family members.

Clarification is required for instances where: (1) physician consent to contact the patient is not required; (2) there is a desire to know from the physician if the patient is well enough to participate if patient has told of diagnosis; and (3) if it is not possible to identify the patient's current physician and direct contact with the patient is necessary. Physicians are not contacted to get their consent for registry usage, they are contacted to see from the physician if the patient is well enough to participate.

Next Steps/Closing Remarks

Mary McBride

Ms. McBride reminded participants that this workshop is part of an ongoing process to develop national guidelines for privacy principles. It is hoped that registries will incorporate some of this information into national consensus guidelines and use it to develop policies of their own. This report will be distributed, and a presentation on the workshop results will be given at the NAACCR Annual Meeting in June. Ms. McBride thanked workshop participants, sponsors, consultants, the facilitator, and the Workshop Planning Committee.

Action Items

The following action items were identified during the workshop:

- Circulate the report from this workshop to participants, receive participant feedback, and incorporate revisions into a revised report for circulation to the NAACCR membership, particularly Canadian registry directors and sponsors.
- Establish a committee, endorsed by the Canadian Council of Cancer Registries, to develop a national consensus set of guidelines for surveillance data access for cancer registries following the privacy principles and the latest Canadian legislation on confidentiality protection, in consultation with the registry directors.
- Have the committee review Mr. Flaherty's draft Privacy Policy/Code for a Canadian Cancer Registry, with the intent of producing a code that could be customized to fit the needs of cancer registries; have the committee review the framework for a Privacy Assessment for Cancer Registries, again so it can be modified for use within individual registries.

APPENDIX A: The 10 Privacy Commandments

1. **Accountability.** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
2. **Identifying Purposes.** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. **Consent.** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where appropriate.
4. **Limiting Collection.** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure, and Retention.** Personal Information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.
6. **Accuracy.** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards.** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness.** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. **Individual Access.** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance.** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

APPENDIX B: Privacy Policy/Code for a Canadian Cancer Registry **(NOTE: Draft: for circulation only with report)**

Assumptions:

1. In the absence of a statutory obligation to comply with the *Personal Information Protection and Electronic Documents Act* (PIPEDA), a cancer registry should still self-regulate for the protection of personal information on employees, patients, donors, and others that is in its custody and control. Self-regulation implies exactly that; there is no legal force behind the “regulations” and no external oversight, such as by the Privacy Commissioner of Canada. Some cancer agencies are, of course, already under the jurisdiction of a provincial or territorial Information and Privacy Commissioner/Ombudsman/Commission on Access to Information (Quebec).
2. The “national standard” for privacy protection can be found in schedule 1 to the PIPEDA as presented below (which applies strictly to commercial uses of personal information in the private sector, including health information, that crosses provincial boundaries for consideration).
3. The Ten Privacy Commandments in schedule 1 of the PIPEDA are used below as a guide to a cancer registry’s self-regulatory effort. These will not replace any statutory, common law, or contractual obligations that are in force with respect to how such an entity collects, uses, and discloses personal information. Although part 1 of the PIPEDA modifies the schedule in a variety of ways, it does not seem necessary to incorporate these changes in this broad-based Privacy Policy (although it is possible to do so). The argument for self-regulation resolves around sound management of the privacy issue and risk avoidance.
4. Unless otherwise required by law, the intent would be to apply this privacy policy only to new data collection by a cancer agency, after it has approved the Privacy Policy and a date is established for its entering into force.
5. For a more detailed commentary on the meaning and intent of the principles set out in Schedule 1 of the PIPEDA, see Stephanie Perrin, Heather H. Black, David H. Flaherty, and T. Murray Rankin, The Personal Information Protection and Electronic Documents Act: An Annotated Guide (Irwin Law, Toronto, 2001), pp. 13-47.
6. **Prepared for illustrative purposes only. Silent editing has occurred throughout, especially of matters that are not relevant to the work of cancer registries.**
7. **Changes made to reflect the special character of cancer registries are noted in italics.**
8. **When cancer registries are governed, at least in part, by provincial/territorial law and policy, then the specific practices could be integrated with this generic policy, especially by noting the legal requirements in the context of this self-regulatory document.**

SCHEDULE I

(Section 5)

A Privacy Policy/Code for a Canadian Cancer Registry (DRAFT)

4.1 Principle 1 - Accountability

A cancer registry is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the cancer registry's compliance with the following principles.

4.1.1

Accountability for the cancer registry's compliance with the principles rests with the designated individual(s), even though other individuals within the cancer registry may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the cancer registry may be delegated to act on behalf of the designated individual(s).

4.1.2

The identity of the individual(s) designated by the cancer registry to oversee the cancer registry's compliance with the principles shall be made known upon request.

4.1.3

A cancer registry is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The cancer registry shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Cancer registries shall implement policies and practices to give effect to the principles, including

- (a) implementing procedures to protect personal information;
- (b) establishing procedures to receive and respond to complaints and inquiries;
- (c) training staff and communicating to staff information about the cancer registry's policies and practices; and
- (d) developing information to explain the cancer registry's policies and procedures.

4.2 Principle 2 - Identifying Purposes

The cancer registry shall define the purposes for which it collects personal information at or before the time the information is collected.

4.2.1

The cancer registry shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows cancer registries to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle (Clause 4.4) requires a cancer registry to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes. *When a cancer registry collects personal information indirectly, it will encourage the original collectors to give such notice.*

4.2.4

When personal information that has *collected directly* is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, cancer registries *like cancer registries* that *sometimes* do not have a direct relationship with the individual may not always be able to seek consent.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, a cancer registry will seek consent for the use or disclosure of the information at the time of *direct* collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when a cancer registry wants to use information for a purpose not previously identified). *When reporting of cancer episodes occurs on a mandatory legal basis, then the cancer registry will endeavor to ensure that the patient receives written notice at the time of original collection.*

4.3.2

The principle requires “knowledge and consent”. Cancer registries shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

A cancer registry shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the cancer registry may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, cancer registries shall take into account the sensitivity of health information.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. [insert an example relevant to a cancer registry, such as a person giving a tissue sample to a lab for analysis; would he or she expect cancer reporting?] In this case, the cancer registry can assume that the individual’s request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which a cancer registry seeks consent may vary, depending on the circumstances and the type of information collected directly. A cancer registry should generally seek express consent when *health information is collected*. Implied consent would generally be appropriate when the information is less sensitive. [modify?] Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

- (a) an application form [what is right term for a cancer patient seeking treatment?] may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;
- (b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to a cancer registry. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;
- (c) consent may be given orally when information is collected over the telephone; or
- (d) consent may be given at the time that individuals use a health service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The cancer registry shall inform the individual of the implications of such withdrawal. *[will need special treatment of historic data on an individual]*

4.4 Principle 4 - Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the cancer registry. Information shall be collected by fair and lawful means.

4.4.1

Cancer registries shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Cancer registries shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent cancer registries from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 Principle 5 - Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes. *[would mean permanent collection in the case of a cancer registry.]*

4.5.1

Cancer registries using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2

Cancer registries should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. A cancer registry may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Cancer registries shall develop guidelines and implement procedures to govern the destruction of personal information. *[not likely to ever happen; indicate that]*

4.5.4

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.6 Principle 6 - Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

4.6.1

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

4.6.2

A cancer registry shall not routinely update personal information, unless such a process is necessary to fulfill the purposes for which the information was collected.

4.6.3

Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

4.7 Principle 7 - Safeguards

Security safeguards appropriate to the sensitivity of the information shall protect personal information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Cancer registries shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

- (a) physical measures, for example, locked filing cabinets and restricted access to offices;
- (b) organizational measures, for example, security clearances and limiting access on a need-to-know” basis; and
- (c) technological measures, for example, the use of passwords and encryption.

4.7.4

Cancer registries shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 Principle 8 - Openness

A cancer registry shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Cancer registries shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about a cancer registry’s policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

- (a) the name or title, and the address, of the person who is accountable for the cancer registry's policies and practices and to whom complaints or inquiries can be forwarded;
- (b) the means of gaining access to personal information held by the cancer registry; *[issue of sending the applicant back to the original collector, such as a hospital]*
- (c) a description of the type of personal information held by the cancer registry, including a general account of its use;
- (d) a copy of any brochures or other information that explain the cancer registry's policies, standards, or codes; and
- (e) what personal information is made available to related cancer registries (e.g., subsidiaries).

4.8.3

A cancer registry may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, a cancer registry may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.

4.9 Principle 9 - Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, a cancer registry may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1

Upon request, a cancer registry shall inform an individual whether or not the cancer registry holds personal information about the individual. Cancer registries are encouraged to indicate the source of this information. The cancer registry shall allow the individual access to this information. However, the cancer registry may choose to make sensitive medical information available through a medical practitioner. In addition, the cancer registry shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2

An individual may be required to provide sufficient information to permit a cancer registry to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, a cancer registry should attempt to be as specific as possible. When it is not possible to provide a list of the cancer registries to which it has actually disclosed information about an individual, the cancer registry shall provide a list of cancer registries to which it may have disclosed information about the individual.

4.9.4

A cancer registry shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the cancer registry uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the cancer registry shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the cancer registry shall record the substance of the unresolved challenge. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

4.10 Principle 10 - Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the cancer registry's compliance.

4.10.1

The individual accountable for a cancer registry's compliance is discussed in Clause 4.1.1.

4.10.2

Cancer registries shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

4.10.3

Cancer registries shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate.

4.10.4

A cancer registry shall investigate all complaints. If a complaint is found to be justified, the cancer registry shall take appropriate measures, including, if necessary, amending its policies and practices.

APPENDIX C: Factors To Consider in Determining When It Is Impracticable To Obtain Consent

- The size of the population being researched
- The proportion of individuals likely to have relocated or died since the time the personal information was originally collected
- The risk of introducing potential bias into the research thereby affecting the generalizability and validity of results
- The risk of creating additional threats to privacy by having to link otherwise de-identified data with nominal identifiers in order to contact individuals to seek their consent
- The risk of inflicting psychological, social, or other harm by contacting individuals or families with particular conditions or in certain circumstances
- The difficulty of contacting individuals directly when there is no existing or continuing relationship between the organization and the individuals
- The difficulty of contacting individuals indirectly through public means, such as advertisements and notices
- Whether, in any of the above circumstances, the requirement for additional financial, material, human, organizational, and other resources needed to obtain such consent will impose an undue hardship on the organization.

APPENDIX D: Web Addresses for Organizations and Documents Discussed at the North of the Border Workshop

Canadian Organization for the Advancement of Computers in Health

- <http://www.coachorg.com>

Canadian Institute for Health Information

- <http://www.cihi.ca>

Canadian Institutes for Health Research

- http://www.cihr.ca/about_cihr/ethics/initiatives_e.shtml

Canadian Standards Association: Model Code for the Protection of Personal Information

- <http://www.csa.ca/standards/privacy/default.asp?load=code&language=English#modelcode>

Centers for Medicare and Medicaid Services

- <http://www.cms.mms.gov>

Centre for Health Services and Policy Research (University of British Columbia)

- <http://www.chspr.ubc.ca>

Health Canada

- <http://www.hc-sc.gc.ca>

Industry Canada/

<http://www.ic.gc.ca>

National Cancer Institute

- <http://www.cancer.gov>

National Cancer Institute of Canada

- <http://ncic.cancer.ca>

National Guideline Clearinghouse

- <http://www.guidelines.gov>

North American Association of Central Cancer Registries

- <http://www.naaccr.org>

North American Association of Central Cancer Registries – Recommendations for Public Use of National Cancer Data

- <http://www.naaccr.org/data/papers/depc.pdf>

Statistics Canada

- <http://www.statcan.ca>

Statistics Canada: Electronic Linkage

- <http://www.statcan.ca/english/about/abtstc.htm>

Surveillance, Epidemiology and End Results Program

- <http://www.seer.cancer.gov>

Treasury Board of Canada: Model Cross-Jurisdictional Privacy Impact Assessment Guide

- http://www.tbs-sct.gc.ca/gos-sog/psgos/impl-rep/impl-rep2000/imp.report75_pia-eiprp_e.htm

Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans

- <http://www.nserc.ca/programs/ethics/english/policy.htm>