

# Regulatory Compliance — September 2100

## Security of Records in Clinical Research

**Smart and Associates**

**Jean Smart, RAC**

Article for CRPBC Newsletter September 1, 2010



When discussing and reviewing the clinical trials security of electronic health records and electronic data capture ("EDCs") systems with organizations and sites involved in clinical research, the two basic issues of *confidentiality* and *privacy* always come up. Within the research sector, these are the key areas from which the *security obligations* originate. Confidentiality and privacy are often confused and are treated interchangeably. It should be noted that they are indeed different, but do have overlapping, rules. To ensure compliance with regulatory authorities and industry; sites and organizations need to have robust policies in place and understand the differences in the terms related to security. The security aspects of a clinical trial are indeed auditable.

### Confidentiality

Confidentiality is a responsibility that health institutions, organizations, professionals and providers simply have. They are obligated to protect and not to disclose patients' or clients' personal health information (PHI) except as expressly permitted (i.e. by consent). For Doctors, nurses and pharmacists in British Columbia, the rules are outlined in their professional codes of practice or practice standards which are overseen by their colleges in applicable provincial legislation designated by the *Health Professionals Act*<sup>1</sup>. Institutions such as hospitals and social agencies are subject to confidentiality obligations contained in provincial *Hospitals Act*<sup>2</sup> and other similar legislation in other jurisdictions.

Most of the legislation pertaining to confidentiality specifies the prohibition against organizations and public boards to allow any person to remove, inspect or receive information from records of personal health information. Professionals involved in clinical research are quite familiar with The *Food and Drug Regulations*<sup>3</sup> pertaining to clinical trials and research which does allow for the authorized inspection of records. Access to these records is required to be specified in both the protocol and in the subject consent form.<sup>4</sup>

While generally there is a prohibition against unauthorized disclosure of PHI in the legislation; it does not directly address security. Clearly, confidentiality implies security; but security *rules* and *standards* constitute a distinct category: essentially they are the means by which confidentiality is to be achieved. So, while confidentiality obligation exists for health providers, it contains no explicit directions or rules that address security, or guidance as to the standard that can be expected. There is obvious obligation and incentive for researchers to adopt appropriate security because there are consequences if confidentiality is breached.

# Regulatory Compliance — September 2100

## Security of Records in Clinical Research

### Privacy Law

The other basic area from which security criteria is derived is privacy law. Privacy law has been in place in Canada since 2001.<sup>5 6</sup> It has been effective in British Columbia (BC) since 2004.<sup>7 8</sup> BC was one of the provinces that 'opted out' and developed its own privacy legislation for both the private and public sectors.

Privacy is distinct from confidentiality because it comes from the *right* of individuals to *control* their personal information, in contrast with the obligation of providers, which is to keep PHI confidential. Maintaining confidentiality is an important aspect of protecting privacy and it is here that the two principles overlap.

Privacy implies security because one of the main privacy principles is that an individual has the right to have any of his or her personal information that is held by a data collector protected from unauthorized disclosure. The privacy law is much more specific than the confidentiality issue in that it expressly identifies a security requirement.

This security requirement is set out in the privacy laws, and it is these laws that form the primary mandate to health care providers and researchers to establish appropriate security systems with respect to PHI both generally and, potentially, specifically with respect to electronic systems. It is important to note that if practitioners or institutions fail to meet this standard, they may be liable in damages to the individuals whose information has been compromised.

The provincial privacy related laws across Canada generally outline some guidance for data collectors that security systems and procedures should be adopted. It requires that a custodian take steps *reasonable in the circumstances* to protect information within its custody or control against theft, loss and unauthorized use or disclosure.<sup>9</sup> There is some additional specific guidance, addressing protection against unauthorized copying, modification or disposal, secure handling and disposal of records. The regulations outline more detailed procedures for records retention procedures, electronic data collection and management and electronic network service providers. To date however, only regulations relating to network service providers have been enacted.<sup>10</sup>

The provinces limited detailed guidance respecting security procedures contrasts with the federal law. The federal law which through its adoption of the CSA Model Code provides an outline of the nature of the protections that should be adopted. At the federal level the *Personal Information Protection and Electronic Documents Act*, (PIPEDA)<sup>11</sup> rule makes clear that such protections should include physical, organizational and technological measures and provides examples of each of these categories. The PIPEDA rule also stipulates that organizations must ensure that their employees are trained in security procedures.

While this specificity of required procedures is not currently found in BC's PIPA it is clear that, in order to comply with the legislation, custodians are *expected* to adopt detailed procedures.

# Regulatory Compliance — September 2100

## Security of Records in Clinical Research

### Other Regulatory Influence

There are no privacy regulations respecting records management or electronic data procedures. While this is recognized as a deficiency in privacy law, research personnel should be aware that it has been addressed by Health Canada when the Food and Drug regulations pertaining to clinical trials were amended in 2001. There is a clear expectation in the amendment that records be managed appropriately and securely.<sup>12</sup> There is also a guidance document (GUID 0068) Records related to clinical trials<sup>13</sup> which is a must read for all personnel involved in clinical research. As well the notes accompanying GUIDE 0068 to the Food and Drug Regulations cross reference PICs Annex 11<sup>14</sup> on Computerized Systems. PICS Annex 11 as adopted by Health Canada and it is the Canadian equivalent of the US CFR 21 part 11 on the electronic records, electronic signatures and validation.<sup>15</sup>

### Security is Critical

Why is security such a critical element of a privacy regime?

Firstly, the elemental concept of privacy implies an individual's control over and in effect ownership of his or her personal information. Recognition of this concept dictates that if that information is entrusted to another person, that person must take appropriate precautions to prevent that information from being misused, lost or stolen. Furthermore, implicitly, a privacy regime recognizes that if personal information is misused, an individual may suffer injury – whether it be financial, psychological or physical. The security rule seeks to prevent such injury. But these are not the reasons why the security and effective compliance measures are important.

The unauthorized disclosure of an individual's personal health information can have significant *injurious impact* – whether it be to the individual's dignity and self-esteem, the perception of his or her place in their family and community, or their workplace status. Clearly, this is the most important reason why personal health information must be protected with secure measures.

### Electronic data capture systems

While electronic data capture systems (EDCs) offer significant advantages to efficient research, they can pose challenges to the security of PHI at the site and organizational level. Locks and pass-keys, though potentially sufficient in a paper-based system, are inadequate in an electronic environment. Further, in a computerized environment the detriment made possible in the event of unauthorized access is magnified. Computerized databases of personally identifiable information are more vulnerable than paper-based systems because they may be accessed, changed, viewed, copied, used, disclosed, or deleted more easily and by many more people than paper-based records.

# Regulatory Compliance — September 2100

## Security of Records in Clinical Research

The potential security risks to information collected and managed through EDC systems used in clinical research are many, but they can be addressed through strong protective technology and rigorous procedures. Evaluation of data flow at the initial study planning stages and prior to starting project development by conducting a project based privacy impact assessment is essential to identify risks and any potential study design flaws.

### Ensuring Security

In many private research organizations and increasing in large public health care entities, privacy and security are identified as distinct reporting responsibilities. While it is recognized that they may overlap in many applications – particularly in the research sector – they can have competing priorities and therefore can potentially be in conflict. This circumstance has been recognized by the Ontario Information and Privacy Commissioner's 2008 report on Smart Systems for Health Agency. It is therefore highly recommended that an organization's privacy and security responsibilities be separated and that distinct policies or procedures should be adopted for each responsibility.

While it is not possible to absolutely ensure security of clinical research records, it is essential that your site and organization has done all that it can to protect the individual's reasonable expectation of privacy and security of personal information in clinical research records.

### Tips for Security of Clinical Research Records

- Develop a Security Policy
- Develop a full set of privacy procedures
- Arrange for Staff education on privacy principles
- Arrange for Staff education on security procedures
- Conduct a Privacy Impact Assessment - site or organization
- Develop a procedure and template for project based privacy impact assessments
- Conduct a Project based PIA for each new study in the early planning stages
- Ensure you know which privacy legislation and regulations apply to your study. (consider provinces, interprovincial, international jurisdictions and private or public and private domains)
- Ensure you know which security related regulations apply to your study.
- Designated P.O. to communicate with staff and keep up to date on privacy legislation and guidelines (check out provincial privacy commissioner website)
- Review your privacy and security policies and procedures annually.

### Other Helpful Resources

Nymity map of Privacy Laws ( [www.nymity.com](http://www.nymity.com) )

Office of the Information and Privacy Commissioner for British Columbia (website - [www.oipc.bc.ca](http://www.oipc.bc.ca) )

# Regulatory Compliance — September 2100

## Security of Records in Clinical Research

**Jean Smart is a regulatory affairs professional specializing in Clinical Compliance. Contact her directly at Smart & Associates.604-612-6372 or [jesmart@telus.net](mailto:jesmart@telus.net)**

### References

- <sup>1</sup> Health Professionals Act RSBC 1996 Chapter 183
- <sup>2</sup> Hospital Act RSBC 1996, chapter 200.
- <sup>3</sup> Canada Food and Drugs Regulations Division 5
- <sup>4</sup> Food and Drugs Regulations Division 5 c05.012 and c05.013
- <sup>5</sup> Canada - Personal Information Protection and Electronic Documents Act (PIPEDA)
- <sup>6</sup> Federal Privacy Act
- <sup>7</sup> BC -Personal Information Protection Act (PIPA)
- <sup>8</sup> BC Freedom of Information and Protection of Privacy Act
- <sup>9</sup> Ontario - S.O. 2004, c.3, Sch. A., s. 12(1).
- <sup>10</sup> Ontario - PHIPA O. Reg. 329/04, s. 6
- <sup>11</sup> PIPEDA S.C. 2000, c. 5
- <sup>12</sup> Food and Drug Regulations Division 5 c.05. 012
- <sup>13</sup> Health Canada GUIDE 0068 Guidance for Records related to Clinical Trials June 15, 2006
- <sup>14</sup> PICS Guide to Good Manufacturing Practice for Medicinal Products Annexes - Annex 11  
Computerized Systems
- <sup>15</sup> US CFR 21 Part 11 Electronic Records, Electronic Signatures and Validation
- <sup>16</sup> Review of the Smart Systems for Health Agency (SSHA): An Electronic Foods and Service  
Provider to Health Information Custodians under the Personal Health Information Protection  
Act, 2004, March 16, 2007