CPR Security Policies at BHS

CPR Security Policies Working Group,
Baptist Health Systems of South Florida

Date : 1998/06/1618 : 27 : 33

Abstract

Security policies for Computerized Patient Record (CPR) are described in this document. The policies consistently reflect legal and liability requirements on privacy, confidentiality, safety, and other security aspects of electronic medical records at Baptist Health Systems of South Florida (BHS). The policies are described in the form that allows deriving low-level access control, quality of confidentiality protection, integrity, safety and other rules for direct usage by enterprise security mechanisms.

1 Introduction

1.1 Purpose of CPR security policies

CPR security policies are to provide explicit requirements to CPR security infrastructure including information systems constituting CPR and environment they exist in. The policies are supposed to reflect ALL legal and liability requirements related to CPR. The policies are used to derive security rules, which are a mapping of the policies into a concrete information technology employed by CPR enterprise. For example, the same security policies are used to derive security rules for information systems that use CORBA security services, and for those systems that use operating system security directly, and so on. Thus the policies have to be written very clearly and precisely to avoid ambiguity, confusion, and misunderstanding.

1.2 How are the policies created

The policies are created by careful examination of ALL legal and liability requirements that are imposed on the CPR enterprise. Since there is no known to us mechanical process of deriving security policies from legal and liability requirements, the policies are produced through drafting such policies, discussing them with involved parties, putting them against an available threat model for the CPR enterprise, and refining the policies.

1.3 How are the policies supposed to be maintained

The policies have to be up to date with CPR legal, liability, and other, if any, requirements. Any requirement changes have to be reflected in the policies if such changes affect the policies.

2 Security Policies

Note: This section will be extended to contain all policies on security of computerized patient records with exact concise wording of the policies and explanatory text to help understanding the intent of each policy.

2.1 CPR Logical View

There are two ways to organize electronic clinical records [1]. The first mirrors a small paper-based healthcare practices; each physician keeps a records in their own computer, and information is passed between physicians in the form of summaries (such as referral and discharge information). The second way provides a (logically) single electronic file, which is created before birth or during the first visit, closed on autopsy, and contain everything of clinical interest about the patient that was collected by the hospital staff. The latter approach is called "patient-based records." BHS CPR architecture is based on this approach.

2.2 Persistence

Policy 1: Information shall be only added to a record. No information shall be deleted from a record until the appropriate time period has expired.

2.3 Access Control

Policy 2: Each identifiable patient record *shall* be associated with an access control list naming the people or groups of people or roles assigned to people who may read information in the record or append information to the record. Access to the record shall be controlled according to the rules in the access control list associated with the record. Access control list for a particular record shall be computable for any moment in past so that the exact list of people who could access record at a particular time can be generated.

2.3.1 Psychotherapist-Patient Privilege

According to Florida Evidence Code [2] section 503, "Psychotherapist-Patient Privilege," a patient, or a particular party representing the patient interests, has a privilege to refuse to disclose any information, and to prevent any other person from disclosing, confidential communications or records made for the purpose of diagnosis or treatment of the patient's mental or emotional condition, including alcoholism and other drug addiction, between the patient and the psychotherapist, or persons who are participating in the diagnosis or treatment under the direction of the psychotherapist. This privilege includes any diagnosis made, and advice given, by the psychotherapist in the course of that relationship.

Policy 3: A patient, or the patient's attorney on the patient's behalf, or a guardian or conservator of the patient, or the personal representative of a deceased patient, or the psychotherapist, but only on behalf of the patient, *shall* be given ability to specify if he/she refuses to disclose, and wants to prevent any other person from disclosing, confidential communications or records made for the purpose of diagnosis or treatment of the patient's mental or emotional condition, including alcoholism and other drug addiction, between the patient and the psychotherapist, or persons who are participating in the diagnosis or treatment under the direction of the psychotherapist. This privilege includes any diagnosis made, and advice given, by the psychotherapist in the course of that relationship.

Policy 4: Information related to diagnosis or treatment of the patient's mental or emotional condition, including alcoholism and other drug addiction, and information exchanged between the patient and the psychotherapist, or persons who are participating in the diagnosis or treatment under the direction of the psychotherapist, *shall not* be disclosed to any other person if the patient refused to disclose such information (as per the previous policy). Exception *shall* be provided:

- For communications relevant to an issue in proceedings to compel hospitalization of a patient for mental illness, if the psychotherapist in the course of diagnosis or treatment has reasonable cause to believe the patient is in need of hospitalization.
- For communications made in the course of a court-ordered examination of the mental or emotional condition of the patient.
- For communications relevant to an issue of the mental or emotional condition of the patient in any proceeding in which the patient relies upon the condition as an element of his or her claim or defense or, after the patient's death, in any proceeding in which any party relies upon the condition as an element of the party's claim or defense.

2.3.2 Testing for Human Immunodeficiency Virus

Florida's General Provisions on Public Health [3], section 4, "Testing for Human Immunodeficiency Virus," prohibits[1] performance of a test "designed to identify the human immunodeficiency virus, or its antigen or antibody, without first obtaining the informed consent of the person upon whom the test is being performed." Consent does not have to be in writing as long as there is documentation in the medical record that the test has been explained and the consent has been obtained. If the person is not competent or has not reached the age of majority,[2] a consent has to be obtained from a legal guardian or other person authorized by law. Also, information regarding measures for the prevention of, exposure to, and transmission of human immunodeficiency virus, should be provided prior to the test to the person tested.

Policy 5: Any test designed to identify the human immunodeficiency virus, or its antigen or antibody shall be performed only after an informed consent of the person upon whom the test is being performed. An informed consent can be obtained from the tested person's legal guardian or other person authorized by law if the tested person is not competent or is otherwise unable to make an informed judgment; or has not reached the age of majority. The consent of the parents or guardians of a minor is not a prerequisite for an examination or treatment for sexually transmissible diseases to any minor.

Informed consent is not required:

1. When testing for sexually transmissible diseases is required by state or federal law, or by rule including the following situations:
   (a) HIV testing pursuant to section 8, "Screening for HIV and sexually transmissible diseases," of Florida's Statutes Chapter 796 of persons convicted of prostitution or of procuring another to commit prostitution.
   (b) Testing for HIV by a medical examiner in accordance with section 11 of Florida's Medical Examiners Act [5].
2. Those exceptions provided for blood, plasma, organs, skin, semen, or other human tissue pursuant to section 0041, "Donation and transfer of human tissue; testing requirements," of Florida's General Provisions on Public Health [3].

[1] Informed consent is not required for specifically defined cases, see below.

[2] The consent of the parents or guardians of a minor is not a prerequisite for an examination or treatment for sexually transmissible diseases to any minor, according to section 30 of Florida's "Control of Sexually Transmissible Disease Act" [4].

3. For the performance of an HIV-related test by licensed medical personnel in bona fide medical emergencies when the test results are necessary for medical diagnostic purposes to provide appropriate emergency care or treatment to the person being tested and the patient is unable to consent, as supported by documentation in the medical record. Posttest counseling is required.
4. For the performance of an HIV-related test by licensed medical personnel for medical diagnosis of acute illness where, in the opinion of the attending physician, obtaining informed consent would be detrimental to the patient, as supported by documentation in the medical record, and the test results are necessary for medical diagnostic purposes to provide appropriate care or treatment to the person being tested. Posttest counseling is required if it would not be detrimental to the patient. This subparagraph does not authorize the routine testing of patients for HIV infection without informed consent.
5. When HIV testing is performed as part of an autopsy for which consent was obtained pursuant to section 4, "Autopsies; consent required, exception," of chapter 872, "Offenses Concerning Dead Bodies and Graves," of Florida's Statutes.
6. When an HIV test is mandated by court order.
7. For epidemiological research pursuant to section 0032, "Epidemiological research," of Florida's General Provisions on Public Health [3], for research consistent with institutional review boards created by 45 C.F.R. part 46, or for the performance of an HIV-related test for the purpose of research, if the testing is performed in a manner by which the identity of the test subject is not known and may not be retrieved by the researcher.
8. When human tissue is collected lawfully without the consent of the donor for corneal removal as authorized by section 9185, "Corneal removal by medical examiners," or enucleation of the eyes as authorized by section 919, "Enucleation of eyes by licensed funeral directors," of Florida's Statutes chapter 732, "Probate Code: Intestate Succession and Wills."
9. For the performance of an HIV test upon an individual who comes into contact with medical personnel in such a way that a significant exposure has occurred during the course of employment or within the scope of practice and where a blood sample is taken from that individual voluntarily by medical personnel for other purposes. "Medical personnel" includes a licensed or certified health care professional; an employee of a health care professional, health care facility, or blood bank; and a paramedic or emergency medical technician as defined in section 23, "Definitions," of Florida's Statutes chapter 401, "Medical Telecommunications and Transportations."
   (a) Prior to performance of an HIV test on a voluntarily obtained blood sample, the individual from whom the blood was obtained shall be requested to consent to the performance of the test and to the release of the results. The individual's refusal to consent and all information concerning the performance of an HIV test and any HIV test result shall be documented only in the medical personnel's record unless the individual gives written consent to entering this information on the individual's medical record.
   (b) Reasonable attempts to locate the individual and to obtain consent shall be made and all attempts must be documented. If the individual cannot be found, an HIV test may be conducted on the available blood sample. If the individual does not voluntarily consent to the performance of an HIV test, the individual shall be informed that an HIV test will be performed, and counseling shall be furnished as provided in this section. However, HIV testing shall be conducted only after a licensed physician documents, in the medical record of the medical personnel, that there has been a significant exposure and that, in

the physician's medical judgment, the information is medically necessary to determine the course of treatment for the medical personnel.

(c) A person who receives the results of an HIV test pursuant to this subparagraph shall maintain the confidentiality of the information received and of the persons tested. Such confidential information is exempt from section 07(1), "Inspection, examination, and duplication of records; exemptions," of Florida's Statutes chapter 119, "Public Records."

10. For the performance of an HIV test upon an individual who comes into contact with medical personnel in such a way that a significant exposure has occurred during the course of employment or within the scope of practice of the medical personnel while the medical personnel provides emergency medical treatment to the individual; or who comes into contact with nonmedical personnel in such a way that a significant exposure has occurred while the nonmedical personnel provides emergency medical assistance during a medical emergency. For the purposes of this subparagraph, a medical emergency means an emergency medical condition outside of a hospital or health care facility that provides physician care. The test may be performed only during the course of treatment for the medical emergency.
   (a) An individual who is capable of providing consent shall be requested to consent to an HIV test prior to the testing. The individual's refusal to consent, and all information concerning the performance of an HIV test and its result, shall be documented only in the medical personnel's record unless the individual gives written consent to entering this information on the individual's medical record.
   (b) HIV testing shall be conducted only after a licensed physician documents, in the medical record of the medical personnel or nonmedical personnel, that there has been a significant exposure and that, in the physician's medical judgment, the information is medically necessary to determine the course of treatment for the medical personnel or nonmedical personnel.
   (c) A person who receives the results of an HIV test pursuant to this subparagraph shall maintain the confidentiality of the information received and of the persons tested. Such confidential information is exempt from section 23, "Definitions," of Florida's Statutes 401, "Medical Telecommunications and Transportations."
11. For the performance of an HIV-related test medically indicated by licensed medical personnel for medical diagnosis of a hospitalized infant as necessary to provide appropriate care and treatment of the infant when, after a reasonable attempt, a parent cannot be contacted to provide consent. The medical records of the infant shall reflect the reason consent of the parent was not initially obtained. Test results and posttest counseling shall be provided to the parent when the parent is located.

Section 4 of Florida's General Provisions on Public Health [3] also requires that HIV test results should be revealed only along with the offer for immediate consultation on the meaning of the test results, discussion of possible needs for additional testing, safety measures to prevent transmission of the virus infection, etc.

Policy 6: Results of the test on human immunodeficiency virus, or its antigen or antibody revealed to the person, upon whom the test was performed, shall be accompanied with the immediate opportunity for individual, face-to-face counseling about:

1. The meaning of the test results;
2. The possible need for additional testing;

3. Measures for the prevention of the transmission of the human immunodeficiency virus infection;
4. The availability in the geographic area of any appropriate health care services, including mental health care, and appropriate social and support services;
5. The benefits of locating and counseling any individual by whom the infected individual may have been exposed to the human immunodeficiency virus infection and any individual whom the infected individual may have exposed to such human immunodeficiency virus infection; and
6. The availability, if any, of the services of public health authorities with respect to locating and counseling any individual described in subparagraph 5.

Telephonic posttest counseling shall be permitted when reporting the HIV test results of a home access HIV test.

Section 4 of Florida's General Provisions on Public Health [3] requires that the identity of any person upon whom a test has been performed and test results to be confidential. The following policy is almost completely cited word by word from paragraph (f) of section 4.

Policy 7: No person who has obtained or has knowledge of a test result pursuant to this section may disclose or be compelled to disclose the identity of any person upon whom a test is performed, or the results of such a test in a manner which permits identification of the subject of the test, except to the following persons:

1. The subject of the test or the subject's legally authorized representative.
2. Any person, including third-party payors, designated in a legally effective release of the test results executed prior to or after the test by the subject of the test or the subject's legally authorized representative. The test subject may in writing authorize the disclosure of the test subject's HIV test results to third party payors, who need not be specifically identified, and to other persons to whom the test subject subsequently issues a general release of medical information. A general release without such prior written authorization is not sufficient to release HIV test results.
3. An authorized agent or employee of a health facility or health care provider if the health facility or health care provider itself is authorized to obtain the test results, the agent or employee participates in the administration or provision of patient care or handles or processes specimens of body fluids or tissues, and the agent or employee has a need to know such information. The department shall adopt a rule defining which persons have a need to know pursuant to this subparagraph.
4. Health care providers consulting between themselves or with health care facilities to determine diagnosis and treatment. For purposes of this subparagraph, health care providers shall include licensed health care professionals employed by or associated with state, county, or municipal detention facilities when such health care professionals are acting exclusively for the purpose of providing diagnoses or treatment of persons in the custody of such facilities.
5. The department, in accordance with rules for reporting and controlling the spread of disease, as otherwise provided by state law.
6. A health facility or health care provider which procures, processes, distributes, or uses:

   (a) A human body part from a deceased person, with respect to medical information regarding that person; or
   (b) Semen provided prior to July 6, 1988, for the purpose of artificial insemination.
7. Health facility staff committees, for the purposes of conducting program monitoring, program evaluation, or service reviews pursuant to chapters 395 and 766 of Florida's Statutes.
8. Authorized medical or epidemiological researchers who may not further disclose any identifying characteristics or information.
9. A person allowed access by a court order.
10. A person allowed access by order of a judge of compensation claims of the Division of Workers' Compensation of the Department of Labor and Employment Security.
11. Those employees of the department or of child-placing or child-caring agencies or of family foster homes, licensed pursuant to s. 409.175, who are directly involved in the placement, care, control, or custody of such test subject and who have a need to know such information; adoptive parents of such test subject; or any adult custodian, any adult relative, or any person responsible for the child's welfare, and if a reasonable attempt has been made to locate and inform the legal guardian of a test result.
12. Medical personnel who have been subject to a significant exposure during the course of medical practice or in the performance of professional duties, or individuals who are the subject of the significant exposure as provided in subitems 10 and 11 of the next policy.

2.4 Accountability

Policy 8: Any access to patient records shall be recorded in such a way that at any time it can be found *who* accessed *what information* in the record *with what type of access* (read, append) at *what time.*

References

[1] Ross J Anderson. Security in clinical information systems. Technical report, British Medical Association, January 1996. http://www.cl.cam.ac.uk/users/rja14/#Med.

[2] State of Florida Statutes, http://www.leg.state.fl.us/citizen/documents/statutes. *Florida Evidence Code*, 1997. Chapter 90.

[3] State of Florida Statutes, http://www.leg.state.fl.us/citizen/documents/statutes. *Public Health: General Provisions*, 1997. Chapter 381.

[4] State of Florida Statutes, http://www.leg.state.fl.us/citizen/documents/statutes. *Control of Sexually Transmissible Disease Act*, 1997. Chapter 384.

[5] State of Florida Statutes, http://www.leg.state.fl.us/citizen/documents/statutes. *Medical Examiners Act*, 1997. Chapter 406.