Rhode Island Department of Health
Three Capitol Hill
Providence, RI 02908-5094

www.health.ri.gov

To: Members of the Community Interested in the:
Rules and Regulations Pertaining to the Regional Health Information Organization and Health Information Exchange (R5-37.7-HIE)

From: Amy Zimmerman, MPH, Chief
Health Information Technology

Date: January 6, 2009

Attached for your review and comment are proposed **draft** ***Rules and Regulations Pertaining to the Regional Health Information Organization (RHIO) and Health Information Exchange (HIE).*** These are new regulations proposed in accordance with the provisions of Public Law 08-171 enacted by the Rhode Island General Assembly on July 2, 2008 that requires the Department of Health to establish safeguards and confidentiality protections for a regional health information exchange in Rhode Island. The provisions of this law take effect on March 1, 2009. These draft regulations have been amended since the public meeting on October 27, 2008. These changes are annotated with "compiler's notes" (see attached).

Because of your interest and expertise in these matters, the Department would appreciate your review of the proposed draft regulations. A second ***informal*** community review meeting has been scheduled on this matter for: **Tuesday, 27 January 2009** at **2:00 p.m.** in the **Beck Conference Room** of the Cannon Building (on the lower level behind the snack bar).

If you have any questions about the proposed regulations, or if you wish to submit written comments in advance of the meeting, please direct them to me: **Amy.Zimmerman@health.ri.gov** or 401-222-1439.

Please feel free to circulate additional copies of this document, as needed, to any interested person. Upon request, for persons with disabilities, copies of these proposed regulations are also available in Braille, large print, audio cassette, and electronic file (computer disk). Contact the Division of Health Services Regulation (401-222-3425 or RI Relay number dial 711) if you need such assistance. For your reference, these proposed regulations also appear on the Department's website**:** **www.health.ri.gov** and the Secretary of State's website: **www.sec.state.ri.us/rules.**

Your participation is appreciated. *Thank you.*

Attachment

RULES AND REGULATIONS PERTAINING TO THE REGIONAL HEALTH INFORMATION ORGANIZATION AND HEALTH INFORMATION EXCHANGE

[R5-37.7-HIE]

STATE OF RHODE ISLAND AND PROVIDENCE PLANTATIONS

DEPARTMENT OF HEALTH

February 2009 (Proposed)

COMPILER'S NOTES:
Proposed Additions: The entire proposed regulation is new in its entirety.
Proposed Deletions: There is no existing regulation to modify.
Statutory language appears in italics.
Additions [vs. 27 October 2008 1st Community Review Draft]: Underlined.
Deletions [vs. 27 October 2008 1st Community Review Draft]: ~~Strikeouts.~~

INTRODUCTION

These *Rules and Regulations Pertaining to the Regional Health Information Organization and Health Information Exchange* [*R5-37.7-HIE*] are promulgated pursuant to the authority conferred under §5-37.7 of the General Laws of Rhode Island, as amended, for the purpose of establishing safeguards and confidentiality protections for the Health Information Exchange (HIE) in order to improve the quality, safety and value of health care, keep confidential health information secure and confidential and use the HIE to progress toward meeting public health goals.

Pursuant to the provisions of §42-35-3(c) of the General Laws of Rhode Island, as amended, the following were given consideration in arriving at these regulations:

(1) Alternative approaches to the regulations; and

(2) Duplication or overlap with other state regulations.

Based on the available information, no known alternative approach, duplication or overlap was identified.

TABLE OF CONTENTS

		Page
Section 1.0	**Definitions**	1
Section 2.0	**General Provisions**	3
2.1	Purpose and Scope	3
2.2	Participation in the Health Information Exchange (HIE)	3
2.3	Rhode Island Regional Health Information Organization (RHIO)	3
2.4	Special Requirements Pertaining To the Health Information Exchange (HIE) and the Rhode Island Regional Health Information Organization (RHIO)	4
2.5	Reconciliation With Other Authorities	5
2.6	Director Approvals	5
2.7	Professional Responsibilities	5
Section 3.0	**HIE Advisory Commission**	5
Section 4.0	**Confidentiality Protections**	6
4.1	Patient's Rights	6
4.2	Disclosure - General Requirements	7
4.3	Exceptions From Confidentiality Protection	7
4.4	Secondary Disclosure	7
4.5	Authorization Form	8
4.6	Release of Confidential Health information In Conjunction With Legal Proceedings	8
Section 5.0	**Security Requirements**	9
5.1	Minimum Security Requirements	9
5.2	Safeguards and Security Measures	9
Section 6.0	**Immunity and Waivers**	10
6.1	Immunity	10
6.2	Waivers Void	10
Section 7.0	**Penalties – Attorneys' Fees For Violations**	11
7.1	Civil Penalties.	11
7.2	Criminal Penalties	11
7.3	Commission of Crime	11
7.4	Attorneys’ Fees	11
Section 8.0	**Severability**	11
Section 9.0	**Incorporation By Reference**	11
References		11

SECTION 1.0 DEFINITIONS

Whenever used in these rules and regulations, the following terms shall be construed as follows:

1.1 ***"Act"*** means Chapter 5-37.7 of the Rhode Island General Laws, as amended, entitled, "The Rhode Island Health Information Exchange Act of 2008."

1.2 ***"Authorized representative"*** means:

(1) A person empowered by the patient participant to assert or to waive the confidentiality, or to disclose or authorize the disclosure of confidential information, as established by this chapter. That person is not, except by explicit authorization, empowered to waive confidentiality or to disclose or consent to the disclosure of confidential information; or

(2) A person appointed by the patient participant to make health care decisions on his or her behalf through a valid durable power of attorney for health care as set forth in RIGL §*23-4.10-2; or*

(3) A guardian or conservator, with authority to make health care decisions, if the patient participant is decisionally impaired; or

(4) Another legally appropriate medical decision maker temporarily if the patient participant is decisionally impaired and no health care agent, guardian or conservator is available; or

(5) If the patient participant is deceased, his or her personal representative or, in the absence of that representative, his or her heirs-at-law; or

(6) A parent with the authority to make health care decisions for the parent's child.

1.3 ***"Authorization form"*** means *the form described in* §4.5 *and by which a patient participant provides authorization for the RHIO to allow access to, review of, and/or disclosure of the patient participant's confidential health information by electronic, written or other means.*

1.4 ***"Business associate"*** means: *a business associate as defined by HIPAA*, and its implementing regulations (45 CFR Parts 160-164).

1.5 ***"Confidential health information"*** means *all information relating to a patient participant's health care history, diagnosis, condition, treatment, or evaluation.*

1.6 ***"Coordination of care"*** means *the process of coordinating, planning, monitoring, and/or sharing information relating to and assessing a care plan for treatment of a patient.*

1.7 ***"Data submitting partner"*** means *an individual, organization or entity that has entered into a business associate agreement with the RHIO and submits patient participants' confidential health information through the HIE.*

1.8 ***"Department"*** means *the Rhode Island Department of Health.*

1.9 ***"Disclosure report"*** means *a report generated by the HIE relating to the record of access to, review of and/or disclosure of a patient's confidential health information received, accessed or held by the HIE.*

1.10 ***"Electronic mobilization"*** means *the capability to move clinical information electronically between disparate health information systems while maintaining the accuracy of the information being exchanged.*

1.11 ***"Emergency"*** means *the sudden onset of a medical, mental or substance abuse or other condition manifesting itself by acute symptoms of severity (e.g. severe pain) where the absence of medical attention could reasonably be expected, by a prudent lay person, to result in placing the patient's health in serious jeopardy, serious impairment to bodily or mental functions, or serious dysfunction of any bodily organ or part.*

1.12 ***"Health care provider"*** means *any person or entity licensed by this state to provide or lawfully providing health care services, including, but not limited to, a physician, hospital, intermediate care facility or other health care facility, dentist, nurse, optometrist, podiatrist, physical therapist, psychiatric social worker, pharmacist or psychologist, and any officer, employee, or agent of that provider acting in the course and scope of his or her employment or agency related to or supportive of health care services.*

1.13 ***"Health care services"*** means *acts of diagnosis, treatment, medical evaluation, referral or counseling or any other acts that may be permissible under the health care licensing statutes of this state.*

1.14 ***"Health Information Exchange"*** or ***"HIE"*** means *the technical system operated, or to be operated, by the RHIO under state authority allowing for the statewide electronic mobilization of confidential health information, pursuant to the Act* and these Regulations.

1.15 ***"HIE Advisory Commission"*** means *the advisory body established by the Department in order to provide community input and policy recommendations regarding the use of the confidential health information of the HIE.*

1.16 ***"HIPAA"*** means *the Health Insurance Portability and Accountability Act of 1996, as amended*, and its implementing regulations (45 CFR Parts 160-164).

1.17 ***"Participant"*** means *a patient participant, a patient participant's authorized representative, a provider participant, a data submitting partner, the regional health information organization and the Department* ~~*of health*~~*, that has agreed to authorize, submit, access and/or disclose confidential health information via the HIE in accordance with* the Act and these Regulations**.**

1.18 ***"Participation" means*** *a participant's authorization, submission, access and/or disclosure of confidential health information in accordance with* the Act and these Regulations**.**

1.19 ***"Patient participant"*** means *a person who receives health care services from a provider participant and has agreed to participate in the HIE through the mechanisms established in the* Act and these Regulations.

1.20 ***"Provider participant"*** means *a pharmacy, laboratory or health care provider who is providing health care services to a patient participant and/or is submitting or accessing health information through the HIE and has executed an electronic and/or written agreement regarding disclosure, access, receipt, retention or release of confidential health information to the HIE.*

1.21 ***"Regional health information organization"*** or ***"RHIO"*** means *the organization designated as the RHIO by the State* of Rhode Island *to provide administrative and operational support to the HIE.*

1.22 "***Regulations" [*"these Regulations"*]*** means all sections of the *Rules and Regulations Pertaining to the Regional Health Information Organization and Health Information*

Exchange [*R5-37.7-HIE*]. Unless specifically cited otherwise, all references contained herein shall be interpreted as pertaining to these Regulations.

1.23 "***RIGL***" means the General Laws of Rhode Island, as amended.

SECTION 2.0 GENERAL PROVISIONS

2.1 **Purpose and Scope.** These Regulations *establish safeguards and confidentiality protections for the* Health Information Exchange (*HIE*) *in order to improve the quality, safety and value of health care, keep confidential health information secure and confidential and use the HIE to progress toward meeting public health goals.*

2.2 **Participation in the Health Information Exchange (HIE):**

(a) *A statewide* Health Information Exchange (*HIE*) has been established pursuant to RIGL §5-37.7 *to allow for the electronic mobilization of confidential health information in Rhode Island. Confidential health information* shall *only be accessed, released or transferred from the HIE in accordance with* the Act, these Regulations, and any other applicable state or federal law or regulation.

(b) *Patients and health care providers shall have the choice to participate in the HIE, as defined by* the Act and these Regulations. Patients shall agree to participate by signing an authorization form provided by the HIE.

However, provider participants shall *continue to maintain their own medical records, meeting the documentation and other standards imposed by otherwise applicable law* and the prevailing community standard of care.

(c) *Participation in the HIE shall have no impact on the content of or use or disclosure of confidential health information of patient participants that is held in locations other than the HIE.*

(d) *Nothing in* the Act or these Regulations *shall be construed to limit, change or otherwise affect entities' rights or obligations to exchange confidential health information in accordance with other applicable laws.*

(e) *The Department is also considered a participant for public health purposes.*

2.3 **Rhode Island Regional Health Information Organization (RHIO).**

(a) *The RHIO shall, subject to and consistent with* the Act and these Regulations *and contractual obligations it has with the State of Rhode Island, be responsible for all administrative, operational, and financial functions to support the HIE, including, but not limited to, implementing and enforcing policies for receiving, retaining, safeguarding and disclosing confidential health information as required by* the Act.

(b) *The RHIO is deemed to be the steward of the confidential health information for which it has administrative responsibility.*

(c) The RHIO shall develop and implement, at a minimum, current policies and procedures, approved annually by the Director, that address the following topics:

(1) Participant enrollment (both health care provider and consumer);

(2) Participant withdrawal of enrollment; ~~and~~

(3) Revocation of patient authorization ~~of~~ for provider access;

(4) Handling participant complaints and inquiries;

(5) ~~*Patient to*~~ The process through which a patient can obtain a copy of his or her confidential health information from the HIE;

(6) ~~*Patient to*~~ The process through which a patient can obtain a copy of the disclosure report pertaining to his or her confidential health information;

(7) ~~*Patient amendment to*~~ That a patient can request to amend his or her own information through the provider participant;

(8) Tiered access to confidential health information (i.e., criteria and controls to obtain varying degrees of access to data maintained by the HIE);

(9) Privacy, confidentiality and security pertaining to access and maintenance of patient data;

(10) Temporary access to HIE data by health care providers that need to treat a person in emergencies or other unanticipated events; and

(11) Participant notification, if required by RIGL §11-49.2 [Rhode Island Identity Theft Protection Act of 2005], regarding a detected~~/suspected~~ breach of the security system of the HIE ~~security~~ that may have resulted in release of ~~confidential health~~ personal information.

2.4 **Special Requirements Pertaining To the Health Information Exchange (HIE) and the Rhode Island Regional Health Information Organization (RHIO).** *Pursuant to* RIGL §5-37.7-4(e), *the HIE and the RHIO have an obligation to maintain, and abide by the terms of, HIPAA-compliant business associate agreements, including, without limitation:*

(a) *The obligations to use appropriate safeguards to prevent use or disclosure of confidential health information in accordance with HIPAA,* RIGL §5-37.3 [Confidentiality of Health Care Communications and Information Act] *and* the Act;

(b) *Not to use or disclose confidential health information other than as permitted by HIPAA,* RIGL 5-37.3 [Confidentiality of Health Care Communications and Information Act] *and* the Act; ~~or~~

(c) *To make any amendment to a confidential health care record that a provider participant so directs and to respond to a request by a patient participant to make an amendment to the patient participant's confidential health care record* in accordance with HIPAA, the Act and these Regulations.

(d) The RHIO shall have written data sharing agreements in place with provider participants who submit data to the HIE. Such agreements shall, at a minimum, contain all required business associate agreement components.

(e) The RHIO shall have written end user agreements in place with provider participants who access data in the HIE. Such agreements shall, at a minimum, describe roles and responsibilities of both the end user and the RHIO regarding appropriate use of the HIE and assuring patient rights in accordance with applicable federal and state law.

2.5 **Reconciliation With Other Authorities:**

(a) *The Department has exclusive jurisdiction over the HIE, except with respect to the jurisdiction conferred upon the Attorney General in* RIGL §*5-37.7-13*.

(b) The Act and these Regulations *shall only apply to the HIE system, and do not apply to any other private and/or public health information systems utilized in Rhode Island, including other health information systems utilized by a health care provider or other organization that provides health care services.*

(c) As the Act and these Regulations *provide extensive protection with regard to access to and disclosure of confidential health information by the HIE, it supplements, with respect to the HIE only, any less stringent disclosure requirements, including, but not limited to, those contained in* RIGL §*5-37.3* [Confidentiality of Health Care Communications and Information Act], *the Health Insurance Portability and Accountability Act (HIPAA)* and its implementing regulations (45 CFR Parts 160-164), *and any other less stringent federal or state law.*

(d) The Act and these Regulations *shall not be construed to interfere with any other federal or state laws or regulations which provide more extensive protection than provided in* the Act and these Regulations *for the confidentiality of health information. Notwithstanding such provision, because of the extensive protections with regard to access to and disclosure of confidential health information by the HIE provided for in* the Act and these Regulations, *patient authorization obtained for access to or disclosure of information to or from the HIE or a provider participant shall be deemed the same authorization required by other state or federal laws including information regarding mental health (the Rhode Island mental health law,* RIGL §*40.1-5-1 et seq.); HIV (Rhode Island general laws section 23-6-17); sexually transmitted disease (*RIGL §§*23-6-17 and 23-11-9); alcohol and drug abuse (*RIGL §*23-1.10-1 et seq., 42 U.S.C.* §*290dd-2) or genetic information (*RIGL §*27-41-53,* RIGL §*27-20-39 and* RIGL §*27-19-44).*

2.6 **Director Approvals**. Any required approval issued by the Director pursuant to the Act and these Regulations shall be in writing and shall only be valid for twelve (12) months from the date of issue. Any policy, form or other document which requires approval by the Director pursuant to the Act and these Regulations shall be resubmitted on an annual basis.

2.7 **Professional Responsibilities**. In accordance with Title 5 of the General Laws, a provider participant that abandons a patient or denies treatment to a patient solely on the basis of the patient's refusal to participate in the HIE may be subject to appropriate disciplinary sanctions by the Director.

SECTION 3.0 HIE ADVISORY COMMISSION

3.1 Pursuant to RIGL §5-37.7-5(c), the Director shall establish a HIE Advisory Commission of no more than seven (7) members *that shall be responsible for recommendations relating to the use of, and appropriate confidentiality protection for, the confidential health information of the HIE, subject to regulatory oversight by the* Department. *The HIE*

Advisory Commission~~, in consultation with the RHIO,~~ shall ~~also~~ be responsible for recommendations to the Department, and in consultation with the RHIO, regarding the use of the confidential health information.

3.2 Pursuant to RIGL §5-37.7-5(c), the Director shall recommend prospective HIE Advisory Commission members to the Governor, subject to the advice and consent of the Senate. The membership of the HIE Advisory Commission shall include one (1) person with experience in ~~HIPPA~~ HIPAA and~~/or Institutional Review Board (IRB) protocols~~ privacy and security of health care information requirements, one (1) person with experience in operations, maintenance and security of complex electronic databases, and no more than ~~two (2)~~ three (3) persons employed by a health care delivery organization, at least one (1) of whom shall be a physician licensed pursuant to RIGL §5-37. The remaining members shall be selected from business professionals and health care consumers whose experience and expertise will facilitate the work of the Commission.

3.3 The Director shall appoint a chairperson for the HIE Advisory Commission.

3.4 HIE Advisory Commission members shall be appointed for a term of two (2) years. A Commission member may be reappointed for an additional term, but shall not be eligible to serve more than ~~three (3)~~ two (2) consecutive terms.

3.5 The HIE Advisory Commission shall meet at least annually and shall not vote on any recommendations regarding the use of confidential health information unless a quorum is present.

3.6 The HIE Advisory *Commission shall report annually to the* Department *and the RHIO, and such report shall be* ~~publicly available~~ *made public*.

3.7 The HIE Advisory Commission shall actively obtain and consider public input on all recommendations prior to submitting them to the Director. All meetings of the HIE Advisory Commission shall be subject to RIGL §42-46 (Open Meetings).

3.8 The Director may recommend to the Governor that any HIE Advisory Commission member be removed for cause, including but not limited to, failure to attend Commission meetings on a regular basis.

SECTION 4.0 CONFIDENTIALITY PROTECTIONS

4.1 **Patient's Rights.** *Pursuant to* the Act and these Regulations, *a patient participant who has his or her confidential health information transferred through the HIE shall have the following rights:*

(a) *To obtain a copy of his/her confidential health information from the HIE;*

(b) To select which provider ~~organization(s)~~ participant(s) can access his/her health care information;

(c) *To obtain a copy of the disclosure report pertaining to his or her confidential health information;*

(d) *To be notified, as required by* RIGL §*11-49.2 [Rhode Island Identity Theft Protection Act], of a breach of the security system of the HIE;*

(e) (1) *To terminate his or her participation in the HIE* at any time *in accordance with* the Act and these Regulations by signing a revocation form in accordance with the revocation policy established by the RHIO and annually approved by the Director*;*

(2) Upon a patient's termination from the HIE, his/her data shall not be accessed by a provider participant for any purpose, including clinical care; *and*

(f) *To request to amend his or her own information through the provider participant.*

4.2 **Disclosure - General Requirements.**

(a) *Except as provided in §4.3, a patient participant's confidential health information may only be accessed, released or transferred from the HIE in accordance with an authorization form signed by the patient participant or the patient's authorized representative.*

(b) *Except as specifically provided by law,* the Act, these Regulations *or use for clinical care, a patient participant's confidential health information shall not be accessed by, given, sold, transferred, or in any way relayed from the HIE to any other person or entity not specified in the patient participant authorization form meeting the requirements of* §4.5 *without first obtaining additional authorization.*

4.3 **Exceptions From Confidentiality Protection:**

(a) *No authorization for release or transfer of confidential health information from the HIE shall be required in the following situations:*

(1) *To a health care provider who believes, in good faith, that the information is necessary for diagnosis or treatment of that individual in an emergency; or*

(2) *To public health authorities in order to carry out their functions as described in* RIGL *Titles 5, 21 and 23, and rules promulgated under those titles. These functions include, but are not restricted to, investigations into the causes of disease, the control of public health hazards, enforcement of sanitary laws, investigation of reportable diseases, certification and licensure of health professionals and facilities, review of health care such as that required by the federal government and other governmental agencies, and mandatory reporting laws set forth in Rhode Island General Laws; and*

(3) *To the RHIO in order for it to effectuate the operation and administrative oversight of the HIE.*

(b) *Nothing contained in* the Act or these Regulations *shall be construed to limit the permitted access to or the release, transfer, access or disclosure of confidential health information described in* §4.3(a) *or under other applicable law* or regulation.

4.4 **Secondary Disclosure.** *Any confidential health information obtained by a provider participant pursuant to* the Act and these Regulations *may be further disclosed by such provider participant with or without authorization of the patient participant to the same extent that such information may be disclosed pursuant to existing state and federal law,*

without regard to the source of the information.

4.5 **Authorization Form:**

(a) *The authorization form for access to, or the disclosure, release or transfer of, confidential health information from the HIE shall, at a minimum, contain the following information in a clear and conspicuous manner:*

(1) *A statement of the need for and proposed uses of that information;*

(2) *A statement that the authorization for access to, disclosure of and/or release of information may be withdrawn at any future time and is subject to revocation;*

(3) A statement *that the patient has the right not to participate in the HIE;*

(4) *The patient's right to choose to:*

(i) *Enroll in and participate fully in the HIE; or*

(ii) *Designate only specific health care providers that may access the patient participant's confidential health information;*

(5) Other information required by the RHIO, in consultation with the Director.

(b) Any request to enroll in the HIE or to withdraw enrollment from the HIE pursuant to §4.5(a)(2) shall be on forms which are provided by the RHIO, ~~consistent with RIGL §5-37.3-4(4)(d),~~ and annually approved by the Director. ~~Instructions for submission to the RHIO/HIE~~ Enrollment and revocation instructions shall be contained on the form, and the form shall be made public.

4.6 **Release of Confidential Health information In Conjunction With Legal Proceedings.** *Confidential health information received, disclosed or held by the HIE shall not be subject to subpoena directed to the HIE or RHIO unless the following procedures have been completed:*

(a) *The person seeking the confidential health information has already requested and received the confidential health information from the health care provider that was the original source of the information; and*

(b) *A determination has been made by the Superior Court upon motion and notice to the HIE or RHIO and the parties to the litigation in which the subpoena is served that the confidential health information sought from the HIE is not available from another source and is either relevant to the subject matter involved in the pending action or is reasonably calculated to lead to the discovery of admissible evidence in such pending action. Any person issuing a subpoena to the HIE or RHIO pursuant to §*4.6 *shall certify that such measures have been completed prior to the issuance of the subpoena.*

(c) *Nothing* in the Act or these Regulations *shall interfere with or impact upon any rights or obligations imposed by the Workers Compensation Act as contained in* RIGL *Title 28, Chapters 29 through 38.*

SECTION 5.0 SECURITY REQUIREMENTS [The provisions of this section shall not take effect until the Department has executed a written transfer of technical responsibility for the HIE to the RHIO.]

5.1 **Minimum Security Requirements.** *The* RHIO and *HIE* shall, *be subject to the following security procedures*:

(a) *Authenticate the recipient of any confidential health information disclosed by the HIE* in accordance with prevailing industry standards and safeguards and *pursuant to* the Act and these Regulations.

(b) *Limit authorized access to personally identifiable confidential health information to persons having a need to know that information. Additional employees or agents may have access to de-identified information.*

(c) *Identify an individual or individuals who have responsibility for maintaining* safeguards and *security procedures for the HIE*, as required by §5.2.

(d) *Provide an electronic or written statement to each employee or agent* of the RHIO *as to the necessity of maintaining the security and confidentiality of confidential health information, and of the penalties provided for* in the Act and these Regulations *for the unauthorized access, release, transfer, use, or disclosure of this information.*

(e) *Take no disciplinary or punitive action against any employee or agent* of the RHIO *for bringing evidence of violation of* the Act and these Regulations *to the attention of any person.*

5.2 **Safeguards and Security Measures.**

(a) The RHIO shall have in place appropriate physical, technical and procedural safeguards and security measures to ensure the technical integrity, physical safety, and confidentiality of any confidential health information in the HIE. These safeguards and security measures shall be in place at all times and at any location at which the RHIO, its workforce members, or its contractors hold or access confidential health information. Such safeguards and security measures shall comply with state and federal confidentiality laws including, without limitation, the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (45 CFR §§160-164) and RIGL §5-37.3 [Confidentiality of Health Care Communications and Information Act].

(b) **Security Framework.** The RHIO shall consider the following framework for the security of confidential health information in the HIE. The framework includes four elements: security management, separation of systems, security monitoring and control, and system assessment. To address the four elements of this framework, the RHIO shall develop appropriate and scalable security standards, policies, and procedures that are suitable for the size and complexity of its organization.

(1) **Security Management.** The RHIO shall address:

(i) Maintenance and effective implementation of written policies and procedures that conform to the requirements of this Section to protect the confidentiality, integrity, and availability of the confidential health information that is processed, stored, and transmitted; and to monitor and improve the

effectiveness of such policies and procedures, and

(ii) Training of the RHIO workforce and RHIO contractors who access or hold confidential health information regarding the requirements of the Act, these Regulations and the RHIO's policies and procedures regarding the confidentiality and security of confidential health information.

(2) **Separation of Systems.** The RHIO shall address:

(i) Maintenance of confidential health information, whether in electronic or other media, physically and functionally separate from any other system of records;

(ii) Protection of the media, whether in electronic, paper, or other format, that contain confidential health information, limiting access to authorized users and sanitizing and destroying such media before disposal or release for reuse; and

(iii) Physical and environmental protection, to control and limit physical and virtual access to places and equipment where confidential health information is stored or used.

(3) Security Control and Monitoring. The RHIO shall address:

(i) Identification of those authorized to have access to confidential health information and an audit capacity to detect unlawful, unauthorized or inappropriate access to confidential health information, and

(ii) Measures to prevent unauthorized removal, transmission or disclosure of confidential health information in the HIE.

(4) Security Assessment. The RHIO shall address:

(i) Periodic assessments of security risks and controls, as determined appropriate by the RHIO, to establish if its controls are effective, to correct any deficiency identified, and to reduce or eliminate any vulnerabilities.

(ii) System and communications protection, to monitor, control, and protect RHIO uses, communications, and transmissions involving confidential health information to and from entities authorized to access the HIE.

SECTION 6.0 IMMUNITY AND WAIVERS

6.1 **Immunity.** *Any health care provider who relies in good faith upon any information provided through the HIE in his, her or its treatment of a patient, shall be immune from any criminal or civil liability arising from any damages caused by such good faith reliance. This immunity does not apply to acts or omissions constituting negligence or reckless, wanton or intentional misconduct.*

6.2 **Waivers Void.** *Any agreement purporting to waive the provisions of* the Act or these Regulations *is declared to be against public policy and void.*

SECTION 7.0 PENALTIES – ATTORNEYS' FEES FOR VIOLATIONS

7.1 **Civil Penalties.** *Anyone who violates the provisions of* the Act and these Regulations *may be held liable for actual and exemplary damages.*

7.2 **Criminal Penalties***:* *Anyone who intentionally and knowingly violates the provisions of* the Act and these Regulations *shall, upon conviction, be fined not more than ten thousand dollars ($10,000) per patient, per violation, or imprisoned for not more than one* (1) *year, or both.*

7.3 **Commission of Crime.** *The civil and criminal penalties in* these Regulations *shall also be applicable to anyone who obtains confidential health information maintained under the provisions of* the Act and these Regulations *through the commission of a crime.*

7.4 **Attorneys' Fees.** *Attorneys' fees may be awarded at the discretion of the Court, to the successful party in any action under* the Act and these Regulations.

SECTION 8.0 SEVERABILITY

8.1 *If any provision of* the Act or these Regulations *is held by a court* of competent jurisdiction *to be invalid, that invalidity shall not affect the remaining provisions of* the Act and these Regulations, *and to this end the provisions of* the Act and these Regulations *are declared severable.*

SECTION 9.0 INCORPORATION BY REFERENCE

9.1 Pursuant to RIGL §42-35-3.2, all state and federal laws and regulations specifically cited in these Regulations are hereby incorporated by reference and are deemed to be part of these Regulations.

REFERENCES:

"Confidentiality of Health Care Communications and Information Act," RIGL §5-37.3
Available online: http://www.rilin.state.ri.us/Statutes/TITLE5/5-37.3/INDEX.HTM

Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 enacted on August 21, 1996. Available online: http://aspe.hhs.gov/admnsimp/pl104191.htm

U.S. Department of Health and Human Services - Subchapter C - Administrative Data Standards and Related Requirements [HIPAA implementation regulations] 45 CFR §§160-164
Available online: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?sid=9ee668e16073c0e4b9ed42cce6db1baf&c=ecfr&tpl=/ecfrbrowse/Title45/45cfrv1_02.tpl