Frequently Asked Questions

Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)[1]

Prepared by the Legal Action Center for the
Substance Abuse and Mental Health Services Administration
U.S. Department of Health and Human Services
Sarah A. Wattenberg, MSW, Project Officer
Contract # OMB0990-0115

This document is an educational document from the Substance Abuse and Mental Health Services Administration (SAMHSA) and the U.S. Department of Health and Human Services. It was prepared by SAMHSA staff, in collaboration with staff from the Office of the National Coordinator for Health Information Technology, and contractors and should not be considered legal advice.

---

[1] Health Information Exchange is a generic term that refers to a number of methods and mechanisms through which information can be exchanged electronically.

FREQUENTLY ASKED QUESTIONS

Q1. Does the federal law that protects the confidentiality of alcohol and drug abuse patient records allow information about patients with substance use disorders to be included in electronic health information exchange systems?

A1. Yes. The federal confidentiality law and regulations (codified as 42 U.S.C. § 290dd-2 and 42 CFR Part 2 ("Part 2")), enacted almost three decades ago after Congress recognized that the stigma associated with substance abuse and fear of prosecution deterred people from entering treatment, has been a cornerstone practice for substance abuse treatment programs across the country. Part 2 permits patient information to be disclosed to Health Information Organizations (HIOs)[2] and other health information exchange (HIE) systems; however, the regulation contains certain requirements for the disclosure of information by substance abuse treatment programs; most notably, patient consent is required for disclosures, with some exceptions.[3]

This consent requirement is often perceived as a barrier to the electronic exchange of health information. However, as explained in other FAQs, it is possible to electronically exchange drug and alcohol treatment information while also meeting the requirements of Part 2.

Q2. What types of providers are covered programs under 42 CFR Part 2 ("Part 2")?

A2. To be a "program" that falls under 42 CFR Part 2, an individual or entity must be federally assisted and hold itself out as providing, and provide, alcohol or drug abuse diagnosis, treatment or referral for treatment (42 CFR § 2.11). A program is "federally assisted" if it is:

1) authorized, licensed, certified, or registered by the federal government;

2) receives federal funds in any form, even if the funds do not directly pay for the alcohol or drug abuse services; or

3) is assisted by the Internal Revenue Service through a grant of tax exempt status or allowance of tax deductions for contributions; or 4) is authorized to conduct business

---

[2] As used in this paper, the term "HIO" means an organization that oversees and governs the exchange of health-related information among organizations according to nationally recognized standards. *See* The National Alliance for Health Information Technology, *Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms*, April 28, 2008, found at http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_848133_0_0_18/10_2_hit_terms.pdf. While the majority of these FAQs relate to HIOs, the principles for applying the Part 2 regulations apply to other methods of health information exchange as well.

[3] Most substance abuse treatment programs are also subject to the HIPAA Privacy Rule. In 2004, the Substance Abuse and Mental Health Services Administration (SAMHSA) issued a guidance that summarizes variance between the two Rules and implementation solutions. That guidance can be found at **http://www.hipaa.samhsa.gov/download2/SAMHSAPart2-HIPAAComparison2004.pdf.**

by the federal government (e.g., certified as a Medicare provider, authorized to conduct methadone maintenance treatment, or registered with the Drug Enforcement Agency (DEA) to dispense a controlled substance used in the treatment of alcohol or drug abuse); or 5) is conducted directly by the federal government.

A different definition of a "program" applies when services are provided by a specialized unit or staff within a general medical facility (or 'mixed use' facility – see FAQ #15). A general medical facility has a Part 2 program if:

1) there is "an identified unit within a medical facility which holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment;" or

2) there are "medical personnel or other staff in a general medical facility whose primary function is the provision of alcohol or drug abuse diagnosis, treatment or referral for treatment and who are identified as such providers." (42 CFR § 2.11 (b), (c))

Most drug and alcohol treatment programs are federally assisted. However, there are for-profit programs and private practitioners that may not receive federal assistance of any kind. These programs and practitioners only see clients who have private health insurance or self-pay. Unless the State licensing or certification agency requires those programs or private practitioners to comply with Part 2, they are not subject to the requirements of 42 CFR Part 2, because they are not federally assisted. States may, however, enact laws requiring compliance with Part 2, and programs should refer to their state laws in these situations. Clinicians who use a controlled substance (e.g., benzodiazepines, methadone or buprenorphine) for detoxification or maintenance treatment of a substance use disorder require a federal DEA registration and become subject to Part 2 through the DEA license. In contrast, a physician who does not use a controlled substance for treatment, such as Naltrexone, and does not otherwise meet the definition of a Part 2 program is not subject to Part 2.

Q3. What patients, and which records and information, are protected by 42 C.F.R Part 2?

A3. The Part 2 regulations "impose restrictions upon the disclosure and use of alcohol and drug patient records which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program." (42 CFR § 2.3(a)) The restrictions on disclosure apply to any information disclosed by a Part 2 program that "would identify a patient as an alcohol or drug abuser ..." (42 CFR §2.12(a) (1))

Under 42 CFR § 2.11:

- **"Patient"** means "any individual who has applied for or been given diagnosis or treatment for alcohol or drug abuse at a federally assisted program."

- **"Records"** mean "any information, whether recorded or not, relating to a patient received or acquired by a federally assisted alcohol or drug program."

- **"Disclose or disclosure"** means the "communication of patient identifying information, the affirmative verification of another person's communication of patient identifying information, or the communication of any information from the records of a patient who has been identified."

- **"Patient identifying information"** means the "name, address, social security number, fingerprints, photographs of similar information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information."

In sum, the information protected by Part 2 is any information disclosed by a Part 2 program that identifies an individual directly or indirectly as having a current or past drug or alcohol problem, or as a participant in a Part 2 program.

Q4. For the purposes of the applicability of 42 CFR Part 2, does it matter how HIOs are structured?

A4. No. HIOs may take any number of forms and perform a variety of functions on behalf of the health care providers and other entities participating in the HIO network.[4] Regardless of the functions performed by the HIO, 42 CFR Part 2 still applies. HIOs may:

- provide the infrastructure to exchange patients' health records among entities participating in the HIO network and facilitate the exchange of patients' electronic health information;

- serve as a data repository that holds or stores patient records supplied by entities participating in the HIO network, and then makes them available for exchange in response to participants' requests for such records;

- provide a record locator service for HIO participants and match individuals to their health records from different locations; or

- review and respond to requests for patient records from HIO participating providers.

Each of these scenarios involves the disclosure of Part 2 information. In some cases, the Part 2 program is disclosing protected information to the HIO, which stores it within the HIO system and then makes it available to HIO affiliated members on request. In other cases, the Part 2 program is disclosing protected information to the HIO, which does not keep it in a repository but rather passes the information along to HIO affiliated members. In either event, the disclosure of Part 2 protected patient information to and through the HIO would only be permitted in ways authorized by Part 2. This means that in non-medical emergency situations, either a patient consent or a Qualified Service Organization Agreement (defined in other FAQs) will need to be in place in order for the Part 2 program

[4] For purposes of these FAQs, entities that participate in an HIO network, including but not limited to participating health care providers, will be referred to as "HIO affiliated members." Participating health care providers may also be referred to as "HIO affiliated health care providers."

to disclose the information to the HIO, and patient consent will be needed to allow the HIO to redisclose the Part 2 information to other HIO affiliated members.

Q5. Does 42 CFR Part 2 permit the disclosure of information without a patient's consent for the purposes of treatment, payment, or health care operations?

A5. Unlike HIPAA, which generally permits the disclosure of protected health information without patient consent or authorization for the purposes of treatment, payment, or health care operations, Part 2, with limited exceptions (i.e., medical emergencies and audits and evaluations), requires patient consent for such disclosures (42 CFR §§ 2.3, 2.12, 2.13).[5] Some types of exchange, however, may take place without patient consent when a qualified service organization agreement (QSOA) exists or when exchange takes place between a Part 2 program and an entity with administrative control over that program.

A qualified service organization (QSO) means a person or organization that:

1) provides services to a [Part 2] program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, medical, accounting or other professional services or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy, and

2) has entered into a written agreement with a program under which that person

   a) acknowledges that in receiving, storing, processing or otherwise dealing with any patient records from the programs, it is fully bound by these regulations; and

   b) if necessary, will resist in judicial proceedings any efforts to obtain access to patient records, except as permitted by these regulations.

Where a Part 2 program has entered into a QSOA with an entity that provides any of the covered services, and where the information exchanged is needed to provide the covered services, patient consent is not required. (42 CFR § 2.11)

In addition, patient consent is not required when information is exchanged within a Part 2 program or between a Part 2 program and an entity that has direct administrative control over the program. When a substance use disorder unit is a component of a larger behavioral health program or of a general health program, specific information about a patient arising out of that patient's diagnosis, treatment or referral to treatment can be exchanged without patient consent among the Part 2 program personnel and with administrative personnel who, in connection with their duties, need to know information (42 CFR § 2.12(c)(3)). Patient information may not be exchanged among all of the programs and personnel that fall under the umbrella of the entity that has administrative control over the Part 2 program. A QSOA would be required to enable information exchange without patient consent in this situation.

---

[5] For a comparison of the HIPAA Privacy Rule and Part 2 provisions, see the SAMHSA guidance at: **http://www.hipaa.samhsa.gov/download2/SAMHSAPart2-HIPAAComparison2004.pdf.**

Q6. Under Part 2, can a Qualified Service Organization Agreement (QSOA) be used to facilitate communication between a Part 2 program and an HIO?

A6. Yes. A QSOA under Part 2, which is similar but not identical to a business associate agreement under §§ 164.314(a) and 164.504(e) of the HIPAA Security and Privacy Rules, is a mechanism that allows for disclosure of information between a Part 2 program and an organization that provides services to the program, such as an HIO. Examples of services that an HIO might provide include holding and storing patient data, receiving and reviewing requests for disclosures to third parties, and facilitating the electronic exchange of patients' information through the HIO network.

Before a Part 2 program can communicate with a Qualified Services Organization – in this case the HIO – it must enter into a two-way written agreement with the HIO. Once a QSOA is in place, Part 2 permits the program to freely communicate information from patients' records to the HIO as long as it is limited to that information needed by the HIO to provide services to the program. The HIO may also communicate with the Part 2 program and share information it receives from the program back with the program. Patient consent is not needed to authorize such communications between the HIO and Part 2 program when a QSOA is in place between the two.

Q7. May information protected by Part 2 be made available to an HIO for electronic exchange?

A7. Information protected by 42 CFR Part 2 may only be made available to an HIO for exchange if:

1) a patient signs a Part 2-compliant consent form authorizing the Part 2 program to disclose the information to the HIO, *OR*

2) a Qualified Service Organization Agreement (QSOA) is in place between the Part 2 program and the HIO.

Q8. If Part 2 information has been disclosed to the HIO, either pursuant to a Part 2-compliant consent form authorizing such disclosure or under a QSOA, may the HIO then make that Part 2 information available to HIO-affiliated members?

A8. An HIO may disclose Part 2 information that it has received from a Part 2 program to HIO affiliated members (other than the originating Part 2 program) only if the patient signs a Part 2-compliant consent form. Patient consent is not needed to authorize such communications between the HIO and Part 2 program when a QSOA is in place between the two.

Q9. How do different HIO patient choice models regarding whether general clinical health information may be disclosed to or through an HIO (e.g., no consent, opt in or opt out) affect the requirements of 42 CFR Part 2?

A9. HIOs have adopted a number of different policies for making general clinical information available to participating members. Some HIOs have adopted a "no consent" model, under which a patient's health information may be disclosed to an HIO and subsequently disclosed by the HIO to its affiliated members for specified purposes without obtaining the patient's consent. Other HIOs have adopted an "opt in" model, in which the patient's information is disclosed to the HIO and subsequently disclosed by the HIO to affiliated members for specified purposes only if the patient has affirmatively agreed to such disclosures. Yet other HIOs have adopted an "opt out" model, in which the patient's information is disclosed to the HIO and subsequently disclosed by the HIO to affiliated members for specified purposes unless the patient has affirmatively declined to participate in such exchange.[6]

Regardless of which model the HIO adopts for exchanging general clinical information, the HIO must still comply with the requirements of 42 CFR Part 2 with respect to Part 2 information. This means that even if an HIO adopts a "no consent" model for other information, the patient's Part-2 compliant consent must be obtained to disclose Part 2 information to or through the HIO. On the other hand, the HIO may impose requirements in addition to 42 CFR Part 2. For example, because an "opt in" model requires affirmative patient consent to participate in the HIO, a Part 2 program may need to obtain patient consent to disclose Part 2 information to an HIO even if the Part 2 program has a QSOA with the HIO.

---

[6]This discussion of patient choice models relies upon definitions presented in "Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis" found on the web page of the Office of the National Coordinator for Health Information Technology at http://healthit.hhs.gov/portal/server.pt?open=512&objID=1147&parentname=CommunityPage&parentid=10&mode=2&in_hi_userid=11113&cached=true . There are variations on these general models, however, the principles with respect to 42 CFR Part 2 apply to all models.

Q10. If an HIO is holding or storing Part 2 patient data through a QSOA, can the HIO redisclose the data coming from the Part 2 program to a third party without patient consent?

A10. Only in very limited circumstances. An HIO may disclose the Part 2 information to a contract agent of the HIO, if it needs to do so in order to provide the services described in the QSOA, and as long as the agent only discloses the information back to the HIO or the Part 2 program from which the information originated. If a disclosure is made by the HIO to an agent acting on its behalf to perform the service, both the HIO and the agent are bound by Part 2, and neither organization can disclose the information except as permitted by Part 2.

The HIO would **not** be allowed to redisclose the information to third parties, including HIO affiliated members (except in a medical emergency, which will be discussed in other FAQs), because the HIO affiliated members are not acting as agents of the HIO, but rather are receiving services provided by the HIO. Consequently, if an HIO wants to redisclose the Part 2 program's records to a participating member, it would need the consent of the patient.

Q11. What are the required elements of a patient consent under Part 2?

A11. A written consent to a disclosure under the Part 2 regulations must be in writing and include all of the following items (42 CFR § 2.31):

1) the specific name or general designation of the program or person permitted to make the disclosure;

2) the name or title of the individual or the name of the organization to which disclosure is to be made;

3) the name of the patient;

4) the purpose of the disclosure;

5) how much and what kind of information to be disclosed;

6) the signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent under § 2.14; or, when required for a patient who is incompetent or deceased, the signature of a person authorized to sign under § 2.15 in lieu of the patient;

7) the date on which the consent is signed;

8) a statement that the consent is subject to revocation at any time except to the extent that the program or person which is to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third party payer; and

9) the date, event or condition upon which the consent will expire if not revoked before. This data, event, or condition must insure that the consent will last no longer than reasonably necessary to serve the purpose for which it is given.

Q12. What must a Part 2 program do to notify the HIO, or any other recipient of Part 2 protected information, that it may not redisclose Part 2 information without patient consent?

A12. Part 2 requires each disclosure made with written patient consent to be accompanied by a written statement that the information disclosed is protected by federal law and that the recipient cannot make any further disclosure of it unless permitted by the regulations. Thus, when information is disclosed electronically, an accompanying notice explaining the prohibition on redisclosure must also be electronically sent. Under 42 CFR § 2.32, the statement must read:

"This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR Part 2). The federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is **NOT** sufficient for this purpose. The federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient."

Q13. Can a single consent form be used to authorize the disclosure of Part 2 information to an HIO, as well as authorize the redisclosure of that information to other identified parties, such as HIO affiliated members?

A13. Yes. Under Part 2, a single consent form can authorize a disclosure of information about a patient to one recipient, such as an HIO, and simultaneously authorize that recipient to redisclose that information to an additional entity or entities (such as other HIO affiliated health care providers identified in the consent form), provided that the purpose for the disclosure is the same. The required statement prohibiting redisclosure must accompany the information disclosed through consent, so that each subsequent recipient of that information is notified of the prohibitions on redisclosure.

Q14. Does Part 2 allow the use of multiple-party consent forms?

A14. Yes. A Part 2 consent form can authorize an exchange of information between multiple parties named in the consent form. The key is to make sure the consent form authorizes

each party to disclose to the other ones the information specified and for the purpose specified, in the consent.

If patients want to authorize all or many members of the HIO to access their Part 2-protected record as well as to exchange information with one another, a multiple-party consent form must comply with all relevant requirements of Part 2, including a list of the names of each person or organization to whom disclosures are authorized, that the parties may disclose to each other, and for what purposes.

Q15. Does Part 2 require the use of original signed consents?

A15. No. While consent under Part 2 must be in writing and nonverbal, "wet" signatures – where the entity obtaining a patient's consent gets the consent form signed by the patient in-person and sends the original, signed consent form to the Part 2 provider – are not necessary. Part 2 does not require programs (or recipients named in the consent) to have a patient's "original" signed consent form in their possession to make disclosures. As long as the program or recipient of the consent acts with reasonable caution, it may accept a facsimile or a photocopy of a consent form. Some electronic health information systems may have, or may be developing, the capacity to obtain electronic consents. An electronic signed consent form would be allowable as well, provided an electronic signature is valid under applicable law.

Q16. Under Part 2, may an HIO release demographic information about Part 2 patients without patient consent?

A16. Yes. However, one must be sure to be in compliance with Part 2, which prohibits the disclosure of patient-identifying information. (42 CFR § 2.11 and § 2.13) Therefore, releasing demographic information would only be allowed under Part 2 if the demographic information does not reveal any information that would identify the person, either directly or indirectly, as having a current or past drug or alcohol problem or as being a patient in a Part 2 program.[7]

---

[7] Additional information about patient-identifying information can be found in the 2004 Substance Abuse and Mental Health Services Administration (SAMHSA) guidance document at **http://www.hipaa.samhsa.gov/download2/SAMHSAPart2-HIPAAComparison2004.pdf.**

Q17. Under Part 2, can an HIO reveal that a patient had an encounter at a mixed use facility (or "general medical" facility – see FAQ #2) as long as the HIO does not reveal that the patient was in the mixed use facility's Part 2 program? A mixed use facility can be defined as a service provider organization that provides substance abuse treatment services as well as other health services such as primary care, dental care, mental health services, social services, etc.

A17. Yes, such a disclosure would be permitted under Part 2 because no information protected under Part 2 – any information that would identify the person, either directly or indirectly, as having a current or past drug or alcohol problem or as being a patient in a Part 2 program – is being disclosed. Part 2 explicitly permits "acknowledgement of the presence of an identified patient in a facility or part of a facility if the facility is not publicly identified as only an alcohol or drug abuse diagnosis, treatment or referral facility, and if the acknowledgement does not reveal that the patient is an alcohol or drug abuser." (42 CFR § 2.13(c)(1))

Q18. Under Part 2, can an HIO use a consent form that provides for disclosure to "HIO members" and refers to the HIO's website for a list of those members?

A18. No. 42 CFR Part 2, § 2.31(a)(2) states that consent forms must include the names of the individuals or organizations who will be the recipients of the Part 2 data. The purpose of this requirement is to ensure that patients are sufficiently informed about the disclosures that will be made under the consent. Many individuals throughout the country still do not have computers or access to the Internet, and many HIO affiliated health care providers do not have the resources to provide patients with access to the Internet at the HIO providers' offices. Thus, Part 2 consents should identify, by attachment if necessary, all the HIO affiliated members that are potential recipients of the Part 2 data.

Q19. Can an HIO use a consent form under Part 2 to allow for the disclosure of information to future HIO affiliated health care providers?

A19. No. If a health care provider joins the HIO after a consent is signed, and the patient later goes to that provider for care, Part 2 would require that the new HIO affiliated health care provider obtain the patient's consent for access to the patient's information. This is consistent with 42 CFR Part 2, §2.31(a)(2) that requires patient consent to include the names of the individuals or organizations that will be the recipients of the Part 2 data.

Q20. Can an HIO use a consent form under Part 2 to allow for the disclosure of information to health care providers who are providing on-call coverage for HIO affiliated health care providers or with whom those affiliated providers consult?

A20. Yes, if those providing on-call coverage and consultation for an HIO affiliated provider are listed on the consent form. (See 42 CFR § 2.31(a)(2) requiring the specific name of the individual or organization to whom disclosure may be made to be included in the consent form.)

Q21. Can a Part 2 patient consent be used to enable multiple disclosures?

A21. Yes. Under a Part 2 patient consent, information may be disclosed multiple times, as long as the consent has not yet expired and the entities to whom the information is to be disclosed, the nature of the information, and the purpose for the disclosure specified in the consent form are still the same. A separate consent form does not need to be obtained each time a disclosure of Part 2 records is made.

Q22. Can a Part 2 program or HIO use a consent form that has no specific expiration date but rather states that disclosure is permitted until consent is revoked by the patient?

A22. No. Under 42 CFR § 2.31, a Part 2 consent form must list the date, event, or condition upon which the consent will expire, if not revoked before. Thus, it is not sufficient under Part 2 for a consent form to merely state that that disclosures will be permitted until the consent is revoked by the patient. It is, however, permissible for a consent form to specify the event or condition that will result in revocation, such as having its expiration date be "upon my death."

Q23. Is "treatment" a sufficient description of the intended purpose of a disclosure on a Part 2 consent?

A23. Yes, it is sufficient for "treatment" to be listed on a consent form as the intended purpose of a disclosure under Part 2. A consent authorizing Part 2 patient information to be included in, or exchanged through, an HIO's system for the purpose of "treatment" would **not** permit that information to be shared or used for other purposes, such as for payment, disease management, or quality improvement activities, among others.

Q24. Under Part 2, can any health care provider make the determination that a medical emergency exists, or must a Part 2 provider make that determination?

A24. Any health care provider who is treating the patient for a medical emergency can make that determination. Under the medical emergency provision in Part 2, §2.51, "patient identifying information may be disclosed to medical personnel who have a need for information about the patient for the purpose of treating a condition which poses an immediate threat to the health of any individual and which requires immediate medical intervention." (42 CFR § 2.51(a)) This provision does not require that the Part 2 program make that determination. Thus, any treating provider who determines that a condition which poses an immediate threat to the health of an individual exists can make the decision to "break the glass" (the term used when a health care provider, in the case of an emergency, gets access to a patient's records without the patient's consent) and gain access to Part 2 records. This includes HIO affiliated health care providers treating an individual in a medical emergency who might seek access to records about a patient that are held in, or made available through, an HIO.

Q25. May a computer system be used to automatically determine whether a medical emergency exists and whether a disclosure of Part 2 data can be made without the patient's consent?

A25. Automated electronic health information systems can be programmed to flag specific patient information for a provider to use in determining whether a medical emergency exists and may be programmed to provide alerts to authorized providers. However, one may not automate the determination of a medical emergency. Part 2 requires medical personnel treating an emergency (the treating provider) to use their professional judgment to determine whether the situation meets Part 2's definition of a medical emergency, defined as a particular condition that poses an immediate threat to the health of any individual and requires medical intervention. Once a medical emergency has been determined, Part 2 information may be disclosed without the patient's consent. (42 CFR § 2.51(a))

Q26. If a medical emergency exists, can the entire Part 2 record be released?

A26. Yes. If there is a medical emergency, Part 2 would allow the entire record to be released through an HIO to a treating provider who indicates that he or she needs access to that information to treat a condition that poses an immediate threat to the health of any individual and requires immediate medical intervention.

Q27. For documentation purposes, if a medical emergency is present, would it be permissible under Part 2 to have treating providers simply check a drop down box signifying the existence of such a medical emergency?

A27. Under Part 2 it is permitted, but not sufficient, for treating providers in a medical emergency to merely check a drop down box to signify that they deem that a medical emergency exists under Part 2's definition. Part 2 requires that when a disclosure is made in connection with a medical emergency, the Part 2 program must document in the patient's record the name and affiliation of the medical personnel receiving the information, the name of the individual making the disclosure, the date and time of the disclosure, and the nature of the emergency. Thus, the same information must be recorded by treating providers in any medical emergency and conveyed to the Part 2 program. Automated electronic systems may be used to generate information necessary for a provider to make a determination of a medical emergency, to enable provider entry of emergency information, and/or to generate a report documenting the emergency. Other laws or legal requirements that are, or may be, applicable to HIO affiliated health care providers have similar requirements for audit trails to document the specifics of "break the glass" incidents, such that it enables review by the relevant privacy officer that such access was proper.

Q28. Under Part 2, may an HIO system make clinical decision support functions (such as showing a patient's medications to clinicians when they write prescriptions, automatically ordering medications, and/or alerting clinicians about potential drug interactions) available to HIO affiliated health care providers in a medical emergency?

A28. Yes. Access without patient consent is permitted for information protected by Part 2 in circumstances that meet Part 2's definition of a medical emergency (42 CFR § 2.51). When a treating provider determines that a true medical emergency exists, the system can show the physician the information that is needed to treat that medical emergency, including revealing Part 2 information. In circumstances not involving a medical emergency, the system could not disclose any Part 2 data to the treating physician in the absence of consent. The system could only tell the provider that a specific consent must be obtained, and it must be set up so that such a notice would not reveal the existence of protected Part 2 information.

Q29. Does the Part 2 definition of medical emergency also include mental health emergencies?

A29. Yes. Part 2 does not distinguish between physical and mental health emergencies. A medical emergency is simply defined as a health emergency affecting any individual that requires immediate medical intervention. (42 CFR § 2.51(a))

Q30. When the HIO keeps an electronic record of a medical emergency, does that fully meet Part 2's requirement to document disclosures made in a medical emergencies in the patient's record?

A30. No. Part 2 requires that when a disclosure is made in connection with a medical emergency, the Part 2 *program* (emphasis added) must document in the patient's record the name and affiliation of the recipient of the information, the name of the individual making the disclosure, the date and time of the disclosure, and the nature of the emergency (42 CFR § 2.51(c)). Thus, data systems must be designed to ensure that the Part 2 program is notified when a "break the glass" disclosure occurs and Part 2 records are released pursuant to a medical emergency. The notification should include all the information that the Part 2 program is required to document in the patient's records. The information about emergency disclosures should also be kept in the HIO's electronic system.

Q31. If an HIO's electronic system makes a disclosure in a medical emergency, would documenting the name of the discloser as "electronically disclosed through the system administered by HIO" meet Part 2's requirement that the name of the person who made the disclosure be documented in the patient's record?

A31. No. Part 2 requires that all the circumstances surrounding a disclosure in a medical emergency situation be immediately documented in writing in order to ensure that all the circumstances surrounding a medical emergency disclosure can be investigated and individuals held accountable for their decisions. The HIO is the vehicle for the disclosure of the Part 2 record but not the decision-maker. Thus, documenting the disclosure as "electronically disclosed through the system administered by the HIO," while technically accurate, does not reveal the information that must be documented under Part 2 – the identity of the individual who determined that the situation was in fact a medical emergency and determined that the patient's records should be released. The name of the person who makes the determination and documentation of disclosure made electronically through a system administered by the HIO should be recorded in the HIO's electronic system.

Q32. If an HIO's electronic system sends Part 2 data in a medical emergency to a printer or fax machine in the emergency room, can "the printer in the emergency department" meet Part 2's requirement to document in the patient's record the name of the person to whom the disclosure was made?

A32. No. Part 2 requires that "[t]he name of the medical personnel to whom disclosure was made and their affiliation with any health care facility" be recorded in order to ensure that all the recipients of the information were authorized to receive that information and used it appropriately. Therefore, the name(s) of the medical personnel who received the information and used it to treat the patient should be recorded. (42 CFR § 2.51(c))

Q33. Once Part 2 information is disclosed in a medical emergency, can that information be redisclosed without obtaining patient consent?

A33. Yes. In contrast to circumstances where information is disclosed through patient consent, if a medical emergency exists Part 2 provisions do not prohibit the redisclosure of Part 2 information once it is released. Consequently, medical personnel treating a patient for a medical emergency who are HIO affiliated providers may download and include in their own records the information they obtained in treating the emergency, and may then re-disclose that information to others without obtaining patient consent. However, all disclosures of information under the regulation must be limited to the information necessary to carry out the purpose of the disclosure (42 CFR § 2.13(a)).

Q34. If a patient has previously refused to consent to the release of his/her Part 2 record to a particular HIO affiliated health care provider, and then the patient is brought to that provider in a bona fide medical emergency situation, can that provider gain access through the HIO to the information without the patient's consent under Part 2?

A34. Yes. Under Part 2, records can be released to a provider (including an HIO affiliated health care provider) treating a patient for a medical emergency even if the patient has previously explicitly stated that he/she does not wish his or her records released to that provider.

Q35. Can an HIO disclose data for Disease Management purposes under Part 2 without patient consent?

A35. No. The HIO may not disclose protected Part 2 information for Disease Management purposes unless the patient specifically authorizes such a redisclosure for that purpose in a consent form that meets Part 2's requirements. It would be helpful for the consent form to explain the term "Disease Management" and even, perhaps, provide examples of how the information might be used.

If a Part 2 program discloses information to the HIO via a QSOA, the HIO would still need to obtain the patient's consent before redisclosing the protected information to any third parties for Disease Management purposes.

A disclosure would be permitted in those rare situations where information disclosed by the HIO for Disease Management purposes does not implicitly or explicitly disclose the information protected by Part 2. An example would be when information is aggregated data that does not reveal that the patient has a drug or alcohol problem or the patient's status as a participant in alcohol or drug treatment.

Q36. Under Part 2, would an HIO be permitted to disclose to an HIO affiliated payer the data of several patients held by the HIO, which may include Part 2 data, in order for the payer to target where interventions could be made with particular patients to improve care and management of disease?

A36. No. An HIO would not be permitted to disclose information protected by Part 2 to payers for any reason, including Disease Management, without a Part 2 consent specifically authorizing disclosure for that purpose.

Q37. If an HIO affiliated health care provi der wishes to gain access to a minor's Part 2 record held by the HIO, may the HIO or provider obtain only the consent of a parent or guardian, or must the minor's consent also be obtained?

A37. Under Part 2, the HIO affiliated provider and/or the HIO (acting for the provider and Part 2 program) must always obtain the minor's consent before the provider can gain access to the minor's Part 2 record (42 CFR § 2.14). Depending on state law, the provider might also need to obtain the parent's or guardian's consent as well. Parental consent for a disclosure is required in addition to the minor's only if the Part 2 program is required by state law to obtain parental consent before providing alcohol or drug treatment to the minor.

In other words, if a state law gives a minor the legal authority to consent to treatment on his/her own, without a parent's or guardian's permission or knowledge, then only the minor's consent is required for the HIO to disclose the minor's information to the HIO affiliated health care provider under Part 2. If state law requires parental consent for the minor to be provided alcohol or drug treatment, then the consent of both the minor patient and the parent or guardian is required before the Part 2 program or HIO can make any disclosures. The minor's written consent must be obtained first in all cases.

Maine Health Information Exchange Privacy and Security Framework[1]

The State of Maine has made great strides in developing policies and procedures to support a public/private secure HIE network. HealthInfoNet (HIN), the designated statewide health information exchange organization, working in collaboration with the State Attorney General, the Office of the State Coordinator for HIT (OSC), and its own private/public Board, has assured that data use agreements, business associate agreements, and vendor contracts have been executed in a manner that is appropriate, legal, and supports the vision of HIE in the State.

HIN has developed privacy and security policies consistent with federal guidance and specific to Maine State Law, to assure the privacy and security of all patient data being exchanged (Appendix D of the approved statewide HIE Strategic and Operational Plane includes HIN's Administrative and Safeguard Policies and Procedures). HIN and the State have been long time participants of the Health Information Security and Privacy Collaborative (HISPC) and have used this participation to review and, where possible, harmonize Maine State Law and Regulations with the goals of HIE. In addition, as a result of the HITECH act and the formation of a legal working group within the Office of the State Coordinator for HIT (OSC), HIN and OSC have been closely collaborating to assure alignment of all HIE polices to the Nationwide Privacy and Security Framework for the Electronic Exchange of Individually Identifiable Health Information[2] as well as federal summaries of laws and regulations pertaining to confidentiality, privacy and security[3]. Moreover the changes in the Health Insurance Portability and Accountability Act (HIPAA) have required a revision in policies such as breach notification. The HIN breach Notification Policy in Appendix D of the Strategic and Operational Plan represents that change.

Finally, as noted above, the OSC and HIN are engaging New Hampshire and the other New England States in interstate HIE planning efforts. Maine has been working closely with New Hampshire to begin addressing differing state laws that may impede appropriate HIE in medical trading areas that cross state borders. Leveraging such work as the "Policy Strategies for Advancing Interstate Health Information Exchange A Report to the State Alliance for e-Health"[4] released by the National Governors Association in October 2009 as well as the support of the New England States Consortium of Systems

---

[1] **This framework describes the privacy and security framework for the State of Maine and HealthInfoNet. Specific detail as to the policies and procedures in place at HealthInfoNet are referenced throughout this document and can be found in Appendix D of the ONC approved Maine Statewide Health Information Exchange Strategic and Operational Plan.**

[2] Nationwide Privacy and Security Framework: http://healthit.hhs.gov/portal/server.pt?open=512&objID=1173&parentname=CommunityPage&parentid=34&mode=2&in_hi_userid=10732&cached=true

[3] Summary of Selected Federal Laws and Regulations Addressing Confidentiality, Privacy and Security: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11113_911059_0_0_18/Federal%20Privacy%20Laws%20Table%202%2026%2010%20Final.pdf

[4] Policy Strategies for Advancing Interstate Health Information Exchange. A Report to the State Alliance for e-Health. October 2009: http://www.nga.org/Files/pdf/0910EHEALTHHIEREPORT.PDF

Organizations (NESCSO), shared project proposals are currently under development across the New England region in collaboration with New York.

As a result of these efforts, agreements and policies are in place in Maine, allowing 16 hospitals, a large group practice, MaineCare and the MCDC to actively exchange patient information today. To achieve statewide HIE scale, the State and HIN will continue to partner in assuring the alignment of state privacy laws and regulations that may impede the electronic sharing of PHI especially for those who need it most. HIN has developed a comprehensive business associate agreement (BAA) for all participants in the statewide HIE. The current HIN BAA is provided in Appendix E of the final Strategic and Operational Plan.

In November 2009, a Legal Working Group (LWG) was created by the HIT Steering Committee to address the Legal and Policy Domain requirements in the State HIT Plan as required by the Office of the National Coordinator for HIT (ONC). Specifically, the group was charged with addressing: privacy and security issues related to HIE within the state, and between states; any plans to analyze and/or modify state laws, as well as communications and negotiations with other states to enable exchange; addressing the development of policies and procedures necessary to enable and foster information exchange within the state and interstate; the use of existing or the development of new trust agreements among parties to the information exchange that enable the secure flow of information; and how the state will address issues of noncompliance with federal and state laws and policies applicable to HIE. The LWG included representatives of National Association of Mental Illness of Maine (NAMI-ME), HIV providers and advocates, the Maine Hospital Association, the Maine Medical Association, Maine Family Planning, the Attorney General's Office, HealthInfoNet, the Maine Civil Liberties Union, and private health attorneys, among others.

Like many states, Maine has state laws that provide heightened privacy protection for certain types of health information, specifically for HIV/AIDS and mental health information. The LWG reviewed laws relevant to the group's charge, including provisions of ARRA/HITECH (including the HIPAA amendments), Maine's General Privacy Law, Maine's HIV Privacy Law, and Maine's Mental Health Privacy Law. There was not unanimous agreement on the LWG's recommendations; and the group agreed that the review and analysis of existing state law is an on-going process. The group did however begin to coalesce around areas that should be addressed to support the use of HIE, either as possible amendments to Maine's privacy laws or as recommended changes in HealthInfoNet's practices (see further reference to these recommendations in the HIE Strategic and Operational Plan). The LWG recommended that the OSC continue working on these issues together with the HIT Steering Committee, and present legislation in the first month of the 125th Legislature in 2011. The LWG also recommended that this work continue through the new committee structure constituted under the HIT Steering Committee (HITSC).

Consistent with the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, HealthInfoNet (HIN) has

implemented privacy and security protections essential to establishing public trust. Moreover, to assure trust in the HIE and the accountability of HIN to these policies, the State of Maine's contract with HIN for the HIE cooperative agreement requires the following:

Privacy and Security of PHI in the Health Information Exchange

a) HIN shall develop and maintain comprehensive privacy and security policies that comply with applicable federal and Maine law, including HIPAA, as supplemented by the HITECH Act; Maine Privacy Law; and Maine's Notice of Risk to Personal Health Data Act. HIN shall operate the HIE in compliance with all applicable federal and Maine laws and regulations.

b) HIN shall make PHI available to Users for the purpose of Treatment and Health Care Operations.

c) HIN shall comply with the participant agreement in effect at the time. HIN shall take reasonable measures to enforce the terms of the participant agreement that obligates each Participant to enforce the privacy and other provisions of the participant agreement with respect to its Users and any other Workforce Member.

d) HIN shall develop, manage and maintain business associate agreements with the Participants. HIN shall abide by its HIPAA Business Associate Agreement, the current form of which is attached hereto. Further, in the event of a Breach involving PHI in its possession or under its control, HIN will abide by the breach notification requirements under all applicable federal and state laws and regulations, including 42 U.S.C. §17932 and any regulations promulgated by the Secretary of the U.S. Department of Health and Human Services thereunder. The parties acknowledge and agree that, an incident involving a person who intentionally acquires, accesses or uses Protected Health Information in a manner that violates the Privacy Rule which compromises the privacy or security of the PHI pursuant to the HITECH Act or the regulations promulgated thereunder, constitutes a Breach.

e) HIN shall conduct regular internal audits for compliance with applicable Maine and federal privacy and security laws and regulations. HIN shall obtain an annual external security audit of the health information exchange system from a recognized, independent technology audit firm.

f) HIN shall maintain User authorization, authentication and audit processes/functionality to manage, validate and document system access by Users.

The contract with HIN also includes the following requirements regarding collaboration with existing and new committee structures:

g) HIN shall collaborate with the Privacy Security and Regulatory Committee established by the OSC to analyze state laws regarding the exchange of clinical health information.

h) HIN shall collaborate with the Consumer Committee established by the OSC to address consumer safety and privacy and security concerns.

i) HIN shall collaborate with the Financial Planning and Sustainability Committee established by the OSC to develop a business and sustainability plan for continuing its statewide operations and provides the OSC with a copy of such plan.

j) HIN shall collaborate with the Quality and Systems Improvement Committee to support initiatives for broad health systems improvements.

k) HIN shall collaborate with the OSC to answer question from consumers about the HIE, including information about the opt-out process.

Finally, the HIN contract includes provisions for leveraging HIE technologies procured to support state government efficiencies. "The standardized statewide master patient index maintained by HIN will support the integration and aggregation of person-centric clinical content received from Participants. In developing the HIE operations, HIN will coordinate with the Maine Department of Health and Human Services (DHHS) to identify opportunities for mutual benefit consistent with strategic and operational informatics plans, such as data-sharing for population management and service and program planning."

These contractual requirements define the relationship between HIN and State Government while allowing flexibility for growth and innovation. Below, the eight principles of the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information are described in reference to the HIE activities in Maine.

Individual Access – Currently access to the HIN systems require that end users (providers) to authenticate in to their local organizational network infrastructure prior to accessing the HIN systems. Upon launching HIN from their internal system they are then again faced with another security level of asking for their passwords.

To authenticate the provider, the HIN system holds usernames and passwords for all participants. Each user is assigned an account ID that will allow them to login 24/7. Once authenticated, the user's access is controlled according to their role (e.g., physician, nurse, pharmacist, administrator, etc.). When accessing a patient for the first time, each user is required to "break the glass" and document their relationship to the patient (primary care provider, consultant, etc.). This relationship is maintained for four days. After four days, users accessing the same patient are required to "break the glass" again. Each step of this process is logged in an Audit table. No shared accounts are allowed in HIN, in order to provide accountability. All access to HIN is granted by HIN through the request of designated security officers at each site.

The user requires a computer with a web browser installed. The user is first required to log into the system with a unique user name and password combination. When login is complete, the user can search for the required patient using either the patient identifier or the patient demographics. Once the patient is found, the record is displayed to the user according to the user's security privileges and the patient's recorded consent.

User audit logs are monitored daily for a number of factors including but not limited to, failed authentication attempts, number of logins, number of patients accessed over a time period, number of accesses of a single patient, patients viewed, name similarities between user and patient, and reason(s) given to view the patient(s). These reports can be called ad hoc through the HealthInfoNet portal via an easy to use Graphical Interface. Each participant has identified at least one security officer at their site that has access to the Ad hoc audit log reporting functionality, to use at their discretion. HealthInfoNet provides logs to sites on an as needed basis; some sites request daily summaries of activity.

Currently HIN does not have in place a mechanism allowing individual (consumer) access to personal, identifiable, health information. This information is available from the provider sites as is required by HIPAA. HIN is currently developing a personal health record (PHR) architecture that will allow consumers to access and view personal health information contained in the HIN clinical data repository and to collect and store personally entered health information. The HIN PHR will be presented to the HIN Consumer Advisory Committee and focus groups convened across four regions of the state in November 2010. The results of the focus groups will be written up and presented to the HIN Board of Directors and OSC as well as the development team in December 2010. HIN's intends to be able to deploy this PHR application by the second quarter of 2011.

As the State Medicaid Health IT Plan (SMHP) has been developed there has been a focus on empowering individuals to exercise control over their personal data. The goal is to establish consent management controls that allow MaineCare members to have more control over their data being collected and used by MaineCare. Currently the SMHP is being finalized with additional information on the planning efforts regarding the consent processes for MaineCare.

Correction – Individuals can dispute the accuracy or integrity of their individual identifiable health information and have erroneous information corrected or their dispute documented if their request is denied. These processes are currently managed by all participating healthcare organizations in the State. As HIN is a "steward" of participant organization data, HIN does not change or manipulate participant organization data beyond mapping local coded data to national standards.

The state SMHP includes mechanisms that allow individual access to their personal, identifiable, health information collected by MaineCare and an ability to dispute the accuracy or integrity of that information. There will be provisions made for MaineCare members to comment on corrections to data that were requested and denied. A plan to allow the general population access to their data for purposes described above is under review by HIN.

Openness and Transparency – A community-based Board of Directors with public and private representation oversees HealthInfoNet (HIN). In addition, the membership of the HIN Consumer Advisory Committee is comprised of citizens, consumer advocates, consumer organizations, legal experts, health educators, privacy officers, public health

professionals, and interested parties with experience and expertise in consumer participation and privacy protection in health information technology systems. A member of the HIN Board chairs the Committee. The Committee has been responsible for reviewing and advising on all policies and procedures related to the confidentiality of the HIN clinical data and the privacy protection for patients. The Committee has addressed HIPAA, State law requirements as well as other federal and State guidelines and initiatives, and public health data laws. This committee has been instrumental in the development of the opt-out provision for patient participation in HIN. The state has also provided the active participation of both the OSC and HIN with the consumer advisory council to assure openness and transparency includes groups affected. All HIN Board and Committee meetings are open to the public. Dates and locations of the meetings are posted on the HIN website and meeting minutes are posted 7 days after each meeting.

The State of Maine has created a public/private Health Information Technology Steering Committee (HITSC) to provide governance over the development and deployment of its Statewide HIE Strategic and Operational Plan. This committee has been meeting monthly since March of 2009. This committee held the responsibility for developing the HIE plan as required by ONC and used town-hall meetings and open distribution processes to get feedback on the plan prior to its submission to ONC for approval. The final plan is posted on the Governor's Office of Health Policy and Finance website and the contact information for the State Coordinator for HIT is provided.

Individual Choice - A consumer consent process for participation in the statewide HIE enables consumers to opt out of the exchange. When a consumer opts out, clinical content on the individual is deleted from the clinical data repository and a flag is set in the system blocking the addition of new clinical data for that individual. An audit process is run daily to assure that there is no clinical information associated with any consumer who has elected to opt out of participation in the exchange.

The contractual arrangement between OSC and HIN also includes the following provisions related to consumer education.

Consumer Education

a) HIN shall organize and engage in an expanded and ongoing program of consumer education about the HIE, including the advantages and risks of participation by consumers in the HIE and the options and process for consumers to opt-out of participation in the HIE. HIN shall coordinate with the OSC, provider organizations, consumer advocacy organizations, business and payer organizations, state agencies and state departments involved in health care and health care delivery.
b) HIN shall create and make available to the OSC and to the public educational materials designed to inform consumers about HIN and to enable them to make a decision as to whether to participate in the HIE. HIN shall maintain consumer opt-out policies that comply with all applicable federal and Maine law. Any modification to HIN's consumer opt-out policies and procedures may occur only after approval by the HIN Board of Directors upon its review of a

recommendation by HIN's Consumer Advisory Committee. The Board of Directors' authority to accept or reject the Committee's recommendation is not limited by this provision. HIN shall use reasonable efforts to comply with such policies. A copy of HIN's opt-out policies and procedures is attached hereto.

c) HIN's education materials shall expressly include the following information:
   i) Reference the right of the consumer to determine whether to participate in HIN;
   ii) Inform the consumer about the purpose and operation and of the HIE, the types of PHI in the HIE and the risks and benefits of participating in HIN;
   iii) Inform the consumer that he/she can receive medical treatment without participating in HIN;
   iv) Provide the contact information to report errors in the clinical data content to HIN; and
   v) Outline the process for opting-out of participation in HIN.

Collection, Use, and Disclosure Limitation - The HIN Participation Agreement (provided in Appendix E of the Statewide HIE Strategic and Operational Plan) sets forth conditions of use of personal identifiable health data by participating providers in the exchange. The agreement specifies access, appropriate use, and responsibilities of providers using the HIE. Consistent with HIPPA, a "break the glass" policy requires providers to establish a treatment relationship with the individual whose record is being viewed. An audit trail is made of all persons that access treatment information. Language contained in the states contract with its vendor specifically identifies the responsibilities of the HIE related to data collection, use and disclosure limitations.

Data Quality and Integrity – Policies, software, and essential personnel are required for a HIE to assure data quality and integrity. HIN uses a mapping system that allows legacy data to be included in the record providing clinical value. By taking advantage of mapping rather than using standard only input, participants ensure that all of their legacy data can continue to be useful.

HIN uses its enterprise master patient index (EMPI) enhanced record-matching logic to address the problem of duplicate records and help prevent duplicates from ever entering the EMPI. This logic has the following capabilities:

- Intelligently compares a multitude of data elements;
- Anticipates possible mistakes and variations in data entry;
- Matches records even when their individual data elements are not exactly the same; and
- Helps overcome the inconsistencies created by variations in registration practices across multiple systems.

When a single identifier, such as an enterprise identification number (EIN) or a facility ID/medical record combination, is not available for a record search, or no exact match for the identifier is found, the EMPI uses probabilistic matching logic rules to examine and compare many different data fields within the record. Before a new record is ever added to the EMPI, the matching logic searches and thoroughly compares the incoming data

with the existing demographic data contained in the EMPI. The matching logic can quickly calculate the probability of a record match and presents the user with the information needed to determine if two records belong to one patient. Matching one patient record to another consists of the following steps:

- Normalizing all incoming data elements;
- Querying the EMPI's patient records and building a candidate list;
- Scoring the candidates to indicate the probability of a record match;
- Sorting the candidates by their scores and arranging them for the user from highest to lowest probability; and
- Returning the best candidate(s) to the user.

HIN has in place security analysts whose functions and responsibilities include safeguarding information and the information system assets against unauthorized use, disclosure, modification, and damage or loss. These analysts manage the authorization of access by end users to the HIN clinical data repository and support routine system audits. They also support the development and maintenance of security related policies and procedures. Database managers also play a critical role by maintaining data content and data quality in core HIN databases including the clinical data set, statewide master person index, and provider index.

Safeguards – To assure trust in the HIE, Maine's contract with HIN specifies the responsibilities and actions expected related to privacy and security of personal health information. HIN has in place audit functions, personnel, and policies described above that provide assurance and protection of personal health information.

All connections to HIN are provided through a port-to-port VPN tunnel. The firewall is in a state of implicit deny, and only access rules created by the discretion of HIN are allowed. There are no direct Internet facing servers. All traffic located in these IPSEC tunnels are encrypted in SSL, as another layer of security. The HIN data center also employs a tipping point device that inspects packet flow at the application layer in order to detect any anomalies. No external programs are allowed to make calls directly to the HIN database, at this time. All servers are located in a datacenter that has appropriate physical and technical barriers to limit access. The current data center meets all SAS 70 requirements, and is annually audited by a third party. (The Statewide HIE Strategic and Operational Plan includes more detail on the specific safeguards in place for PHI being exchanged)

Accountability – HIN includes multiple accountability mechanisms to assure that data is shared appropriately and that monitoring mechanisms are in place to mitigate inappropriate and nefarious use, system access, and breach. HIN conducts weekly audits of general system use and daily review of audit logs as described above. HIN also employs continuous automated identification of potentially inappropriate events. When such events occur, the event is flagged and appropriate staff members are identified on a 24 /7 basis. In addition, bi-annually, HIN uses an independent national organization to conduct a system wide attack to identify potential systemic security weaknesses. HIN's policies and procedures as defined in the Statewide HIE Strategic and Operational plan in

Appendix D outline all the specific policies and procedures as related to HIPAA and other Federal and State laws and regulations.

The State's contract HIN includes a number of accountability provisions including strict monitoring of the performance of contract terms and imposing a 10% holdback should the vendor not perform to contract.