New York State Legal Analysis by Scenario

Appendix H to NYS Final Assessment of Variations
and Analysis of Solutions Report

Subcontract No. 36-321-0209825
RTI Project No. 9825

Prepared by:
NYS Department of Health
Manatt, Phelps & Phillips

Submitted to:
Linda Dimitropoulos, Project Director
Privacy and Security Solutions for
Interoperable Health Information Exchange

Submission to RTI: March 30, 2007

Table of Contents

The following is an analysis of the New York State laws as they pertain to the RTI scenarios of the Health Information Security and Privacy Collaboration project. The document discusses provisions under New York law that have been identified by the legal committee as relevant to the scenarios and domains described. Domains have been omitted where no relevant provision of state law was identified under the scenario presented. This document is not legal advice, nor is it intended to be legal advice, nor does it represent the official position of the Department of Health with respect to application and enforcement of state law and regulation on actual, non-hypothetical situations.

1. Patient Care Scenario A

Patient X presents to emergency room of General Hospital in State A. She has been in a serious car accident. The patient is an 89-year-old widow who appears very confused. Law enforcement personnel in the emergency room investigating the accident indicate that the patient was driving. There are questions concerning her possible impairment due to medications. Her adult daughter informed the ER staff that her mother has recently undergone treatment at a hospital in a neighboring state and has a prescription for an antipsychotic drug. The emergency room physician determines there is a need to obtain information about Patient X's prior diagnosis and treatment during the previous inpatient stay.

Note: We assume for purposes of this analysis that New York is the neighboring state. We are also assuming for purposes of this analysis that the hospital in the neighboring state is a mental health facility licensed under Article 31 of the New York Mental Hygiene Law.

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include: (1) the assignment of a unique identifier that is assigned in a confidential manner; and (2) certification in writing by the hospital and the user that the unique identifier is confidential and available only to the authorized user. *10 N.Y.C.R.R. § 405.10(c)(4)(i) and (ii)*.

Discussion

The requirement under New York law that hospitals assign each system user a unique identifier is consistent with HIPAA. See *45 C.F.R. § 164.312(a)(2)(i)*.

The assignment by the hospital of a unique user identifier to each doctor at the General Hospital in State A would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access. *10 N.Y.C.R.R. § 405.10(c)(4)(iv)*.

Hospitals must have procedures in place to modify or terminate use of an assigned identifier due to misuse or changes in the user's employment or affiliation with the hospital. *10 N.Y.C.R.R. § 405.10(c)(7)*.

Discussion

The requirement under New York law that hospitals have policies and procedures to restrict access to appropriately authorized individuals is consistent with HIPAA. See *45 C.F.R. §§ 164.308(a)(3)(i)(C), (4)(ii)(B) and (C)*. The requirement under New York law that hospitals adopt procedures to modify or terminate a system user's access rights based on the termination or modification of the user's relationship with the hospital is also consistent with HIPAA. See *45 C.F.R. § 164.308(a)(3)(ii)(C)*.

The hospital would appear to satisfy New York law if it adopts written policies and procedures identifying the health care organizations that have access to the hospital's medical records and the nature of their access and terminating the organizations' access rights under appropriate circumstances.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 3

Domain Description

Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).*

Discussion

The general duty of hospitals to keep records confidential prohibits hospitals from releasing patient information to out of state entities unless the patient and provider status can be verified. This is consistent with HIPAA which requires covered entities to verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information, if the identity or any such authority of such person is not known to the covered entity. *45 C.F.R. § 514(h).*

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 5

Domain Description

Information protections so that electronic personal health information cannot be improperly modified.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Hospitals are required to conduct audits to track access by system users. *10 N.Y.C.R.R. § 405.10(c)(4)(v)*. Public Health Law § 18(6) also requires the tracking and documentation by licensed professionals and facilities of certain disclosures to third parties (including initial disclosures to government and private payers). Either a copy of the subject's written authorization or the name of and address of such third party and a notation of the purpose of the disclosure must be indicated in the patient's file. Exceptions exist for facility staff and contractors, and government agencies for the purposes of facility inspections or professional conduct investigations.

Discussion

The requirement under *10 N.Y.C.R.R. § 405.10(c)(4)(v)* that hospitals conduct audits to track access by system users does not impose any specific obligations regarding the timing or nature of the mandated audits and is consistent with HIPAA. See *45 C.F.R. § 164.312(b)*. Periodic audits of the access to the hospital's records by other health care organizations would appear to satisfy New York law.

However, Public Health Law § 18(6) law requires additional tracking of disclosures by licensed professionals and facilities than is required under HIPAA. This provision requires tracking of disclosures made to external parties (including providers) not under contract with the disclosing provider, for initial payment disclosures to payers and for other disclosures not explicitly exempted in the law.

Key Legal Barriers

New York law requires additional administrative logging for disclosures by licensed providers beyond HIPAA mandates.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Hospitals must employ safeguards to ensure the security and confidentiality of their medical records. *10 N.Y.C.R.R. § 405.10(c)(4)*.

Hospitals must adopt policies and procedures to ensure the security of electronic or computer equipment from unwarranted access. *10 N.Y.C.R.R. § 405.10(c)(4)(iii)*.

Discussion

The requirement under New York that hospitals employ safeguards to ensure the confidentiality and security of their medical records is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. The requirement under New York law that hospitals adopt policies and procedures to prevent unwarranted access to computer equipment is consistent with HIPAA. See *45 C.F.R. §§ 164.308, 164.310*.

The implementation of HIPAA-compliant safeguards, policies and procedures would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).* This regulation requires hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes. See also, *Williams v. Roosevelt Hospital, 66 N.Y.2d 391(1985)*. Physicians also are prohibited from disclosing identifiable information without consent, except if authorized or required by law. *Education Law §6530(23) and 8 N.Y.C.R.R. § 29.* Such state required consent may be a general consent permitting certain types of disclosures, and the consent does not have to be as specific as a HIPAA authorization or contain all of the HIPAA-mandated elements. If consent is oral or implied, it should be documented in the chart to enable enforcement and minimize litigation risk.

New York law permits medical services to be rendered without consent when in the physician's judgment an emergency exists and the person is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the person's life or health. *N.Y.P.H.L § 2504(4).* This provision has been interpreted to allow release of medical information under such circumstances, as well.

Hospitals operating mental health facilities licensed under Article 31 of the New York Mental Hygiene Law may disclose clinical records of such facilities without the patient's consent only for certain specifically defined purposes. Although the law does not expressly address the issue, the New York State Office of Mental Health ("OMH") is likely to take the position that mental health facilities may not rely on a general consent for the release of such records. OMH has developed a standard consent form for mental health facilities. With the consent of the patient or someone authorized to act on the patient's behalf, clinical records can be released to "persons and entities who have a demonstrable need for such information... provided that disclosure will not reasonably be expected to be detrimental to the patient." *N.Y. Mental Hygiene Law § 33.13(c)(7)*. New York law also provides that clinical records may be released to "appropriate persons and entities when necessary to prevent imminent serious harm to the patient or client or another person." *N.Y. Mental Hygiene Law § 33.13(c)(9)(v)*. NOTE: Psychiatric care and medication is very often provided to patients on general in-patient units in non-OMH licensed hospitals. Such information is governed by the Department of Health (DOH) statutes and regulations applying to general medical information (i.e., 10 N.Y.C.R.R. § 405.10).

Discussion

The New York law requirement that hospitals obtain a general consent prior to releasing medical records is not relevant in this scenario because the hospital in question is a mental health facility licensed under Article 31 of the New York Mental Hygiene Law. Mental health facilities or units in general hospitals which are licensed by Office of Mental Hygiene (OMH) must obtain a standard consent that has been developed in conjunction with OMH unless the disclosure falls under a limited group of exceptions.

In this scenario, New York law is more stringent than HIPAA because the requested disclosure would require a specific mental health consent. Such disclosures are permitted under HIPAA without patient consent or authorization. See *45 C.F.R. § 164.506(c)(2)*.

New York law does provide an exception for a mental health facility licensed by OMH to disclose information to another mental health facility licensed by OMH for treatment purposes. However, since the requested disclosure here is to the emergency room physician of a general hospital in a different state, the exception does not apply.

Another exception that could apply in this scenario is the "imminent serious harm" exception mentioned above. If the mental health facility concludes that disclosure is necessary to

prevent imminent serious harm to the patient or another person, then it could disclose the prior diagnosis and treatment information without the patient's consent. However, it is unclear how this exception is interpreted and a narrow interpretation is unlikely to support disclosure in this scenario.

It is unlikely that the mental health facility already has a consent that would allow disclosure of the patient's diagnosis and treatment. Thus the facility would not be able to agree to the information request from the neighboring state without obtaining a consent unless it believed that such information was necessary to prevent imminent serious harm.

Key Legal Barriers

The mental health facility would not be able to disclose the patient's prior diagnosis and treatment without either (i) obtaining from the patient the standard consent for mental health facilities or (ii) concluding that the disclosure is necessary to prevent imminent serious harm.

4. Patient Care Scenario D

Patient X is HIV positive and is having a complete physical and an outpatient mammogram done in the Women's Imaging Center of General Hospital in State A. She had her last physical and mammogram in an outpatient clinic in a neighboring state. Her physician in State A is requesting a copy of her complete records and the radiologist at General Hospital would like to review the digital images of the mammogram performed at the outpatient clinic in State B for comparison purposes. She also is having a test for the BrCa gene and is requesting the genetic test results of her deceased aunt who had a history of breast cancer.

Note: We assume for purposes of this analysis that New York is State B and that the New York outpatient clinic is run by a hospital licensed under Article 28 of the New York Public Health Law. We also assume that the genetic test results of the patient's deceased aunt are in the custody of the hospital in New York.

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include: (1) the assignment of a unique identifier that is assigned in a confidential manner; and (2) certification in writing by the hospital and the user that the unique identifier is confidential and available only to the authorized user. *10 N.Y.C.R.R. § 405.10(c)(4)(i) and (ii)*.

Discussion

The requirement under New York law that hospitals assign each system user a unique identifier is consistent with HIPAA. See *45 C.F.R. § 164.312(a)(2)(i)*.

The assignment by the hospital of a unique user identifier to each doctor at the General Hospital in State A, and to the patient if the patient is granted access, would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access. *10 N.Y.C.R.R. § 405.10(c)(4)(iv)*.

Hospitals must have procedures in place to modify or terminate use of an assigned identifier due to misuse or changes in the user's employment or affiliation with the hospital. *10 N.Y.C.R.R. § 405.10(c)(7)*.

Hospitals must have procedures for handling requests by other parties for confidential HIV-related information. *10 N.Y.C.R.R. § 63.9(e).*

Discussion

The requirement under New York law that hospitals have policies and procedures to restrict access to appropriately authorized individuals is consistent with HIPAA. See *45 C.F.R. §§ 164.308(a)(3)(i)(C), (4)(ii)(B) and (C)*. The requirement under New York law that hospitals adopt procedures to modify or terminate a system user's access rights based on the termination or modification of the user's relationship with the hospital is also consistent with HIPAA. See *45 C.F.R. § 164.308(a)(3)(ii)(C)*.

The hospital would appear to satisfy New York law if it adopts written policies and procedures identifying the health care organizations and individuals, if any, that have access to the hospital's medical records and the nature of their access and terminating the organizations' and individuals' access rights under appropriate circumstances.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 3

Domain Description

Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).*

Discussion

The general duty of hospitals to keep records confidential prohibits hospitals from releasing patient information to out of state entities unless the patient and provider status can be verified. This is consistent with HIPAA which requires covered entities to verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information, if the identity or any such authority of such person is not known to the covered entity. *45 C.F.R. § 514(h).*

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 5

Domain Description

Information protections so that electronic personal health information cannot be improperly modified.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Hospitals are required to conduct audits to track access by system users. *10 N.Y.C.R.R. § 405.10(c)(4)(v)*. Public Health Law § 18(6) also requires the tracking and documentation by licensed professionals and facilities of certain disclosures to third parties (including initial disclosures to government and private payers). Either a copy of the subject's written authorization or the name of and address of such third party and a notation of the purpose of

the disclosure must be indicated in the patient's file. Exceptions exist for facility staff and contractors, and government agencies for the purposes of facility inspections or professional conduct investigations.

Discussion

The requirement under *10 N.Y.C.R.R. § 405.10(c)(4)(v)* that hospitals conduct audits to track access by system users does not impose any specific obligations regarding the timing or nature of the mandated audits and is consistent with HIPAA. See *45 C.F.R. § 164.312(b)*. Periodic audits of the access to the hospital's records by other health care organizations would appear to satisfy New York law.

However, Public Health Law § 18(6) law requires additional tracking of disclosures by licensed professionals and facilities than is required under HIPAA. This provision requires tracking of disclosures made to external parties (including providers) not under contract with the disclosing provider, for initial payment disclosures to payers and for other disclosures not explicitly exempted in the law.

Key Legal Barriers

New York law requires additional administrative logging for disclosures by licensed providers beyond HIPAA mandates.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Hospitals must employ safeguards to ensure the security and confidentiality of their medical records. *10 N.Y.C.R.R. § 405.10(c)(4)*.

Hospitals must adopt policies and procedures to ensure the security of electronic or computer equipment from unwarranted access. *10 N.Y.C.R.R. § 405.10(c)(4)(iii)*.

Health care providers and health care facilities must adopt protocols for ensuring that records (including electronic records) containing HIV-related information are maintained securely and used for appropriate purposes. *10 N.Y.C.R.R. § 63.9(d)*.

Discussion

The requirement under New York that hospitals employ safeguards to ensure the confidentiality and security of their medical records is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. The same is true of the requirement under New York law that protocols be adopted to ensure records containing HIV-related information are securely maintained and appropriately used. The requirement under New York law that hospitals adopt policies and procedures to prevent unwarranted access to computer equipment is consistent with HIPAA. See *45 C.F.R. § 164.310*.

The implementation of HIPAA-compliant safeguards, policies and procedures would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond HIPAA requirements.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).* This regulation requires hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes. See also, *Williams v. Roosevelt Hospital, 66 N.Y.2d 391(1985)*. Physicians also are prohibited from disclosing identifiable information without consent, except if authorized or required by law. *Education Law §6530(23) and 8 N.Y.C.R.R. § 29.* Such state required consent may be a general consent permitting certain types of disclosures, and the consent does not have to be as specific as a HIPAA authorization or contain all of the HIPAA-mandated elements. If consent is oral or implied, it should be documented in the chart to enable enforcement and minimize litigation risk.

New York law permits medical services to be rendered without consent when in the physician's judgment an emergency exists and the person is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the person's life or health. *N.Y.P.H.L § 2504(4).* This provision has been interpreted to allow release of medical information under such circumstances, as well.

Health care providers may not disclose confidential HIV-related information without the patient's authorization except for certain specifically defined purposes. *N.Y. Public Health Law Article 27-F*. Confidential HIV-related information is defined as information in a health care provider's possession or obtained through a release of such information concerning whether a person has been subject to an HIV test, has an HIV infection, is being treated for an HIV-related illness, or any information that identifies or reasonably could identify the person as having one or more such conditions. *N.Y. Public Health Law § 2780(7).*

If the patient authorizes a release, the health care provider may release the information to whomever the patient directs. *N.Y. Public Health Law § 2782(1)(b).* However, the provider may not rely on a general consent from the patient but must obtain a special HIV release that expressly references the nature of the information being disclosed and contains certain mandated elements. *N.Y. Public Health Law § 2780(9).* The specific release form must be developed by DOH or approved by DOH. *10 N.Y.C.R.R. § 63.5(a)*.

There are exceptions to the general non-disclosure rule that go beyond cases where the patient has given consent to specifically release HIV information. A special HIV consent to disclosure form is not required for disclosure to a "health care provider" or "health facility" when knowledge of the HIV information is necessary to provide appropriate care or treatment to the person whose record contains HIV-related information. *N.Y. Public Health Law § 2782(1)(d); 10 N.Y.C.R.R. § 63.6(a)(4)*. In such cases, a general consent is sufficient. "Health care provider" is defined broadly to include any physician or any other person involved in providing medical, nursing, counseling or other health care services. *N.Y. Public Health Law § 2780(13)* "Health facility" is defined to include any hospital as such term is defined elsewhere in the Public Health Law as "a facility or institution engaged principally in providing

services by or under the supervision of a physician." *N.Y. Public Health Law § 2780(12); N.Y. Public Health Law § 2801(1).*

New York law requires that genetic test results are treated confidentially and not disclosed without the written informed consent of the person tested except in limited circumstances involving court orders and the testing of infants for certain diseases. *N.Y. Civil Rights Law § 79-1(3), (4)(c).* Once a person is deceased, the right of the deceased person to access his or her own medical records may be exercised by a personal representative (a technical term under New York's estates, powers and trusts law) or by a distributee of any deceased person for whom no personal representative has been appointed. *N.Y. Public Health Law § 18(1)(g)*.

A treating provider must release the medical records , including original mammograms of a patient to another provider "upon the written request" of the patient. *N.Y. Public Health Law § 17*.

Discussion

New York law is more stringent than HIPAA because it requires patient consent for the disclosure of protected health information by hospitals to health plans for reimbursement or other payment-related purposes. Such disclosures are permitted under HIPAA without patient consent or authorization. See *45 C.F.R. § 164.506(c)*.

New York law would require the hospital to obtain a general consent from the patient prior to releasing her complete records to the doctor and the digital images of her mammogram to the radiologist at the hospital in State A. Most New York hospitals obtain a general consent from each patient as part of the admission or registration process so it is possible the hospital already has what it needs, but the language in the consent form may be narrowly tailored to permit the hospital to submit bills to the patient's insurer. Thus, the hospital could carefully review its consent form to determine whether the language is sufficiently broad to permit the disclosure requested here or require a new written request for the disclosure. See *N.Y. Public Health Law § 17.*

In addition, since the patient here is HIV positive, it is highly likely that her complete medical records contain confidential HIV-related information so that the outpatient clinic could not release her medical records to the hospital in State A without a specific HIV release from the patient, unless the outpatient clinic determined that release of her records to the hospital was necessary to provide her with appropriate care or treatment, in which case, a general release would suffice. The radiologist's request for the digital images of her last mammography are unlikely to fall under the HIV provisions because those images are unlikely to fall under the definition of confidential HIV-related information.

As to genetic tests, New York law is no more restrictive than HIPAA, which requires compliance with respect to protected health information for deceased individuals and states that if, under applicable law, an executor, administrator or other person has authority to act on behalf of a deceased individual (or the estate thereof), that person is a personal representative with respect to protected health information relevant to the personal representation. *See 45 C.F.R. 164.502(f), (g)(4).* Unless the patient is the personal representative of her deceased aunt, she cannot gain access to the genetic tests of the deceased aunt.

Key Legal Barriers

The hospital might have to revise its standard consent form to cover the provision of access to the EHR to the hospital in State A. In addition, for the complete medical records request, the hospital would have to obtain a special consent from the patient authorizing the release of HIV-related information in her records unless the hospital makes a determination that the release is necessary for the patient's care.

5. Payment Scenario

X Health Payer (third party, disability insurance, employee assistance programs) provides health insurance coverage to many subscribers in the region the health care provider serves. As part of the insurance coverage, it is necessary for the health plan case managers to approve/authorize all inpatient encounters. This requires access to the patient health information (e.g., emergency department records, clinic notes, etc.).
The health care provider has recently implemented an electronic health record (EHR) system. All patient information is now maintained in the EHR and is accessible to users who have been granted access through an approval process. Access to the EHR has been restricted to the health care provider's workforce members and medical staff members and their office staff.
X Health Payer is requesting access to the EHR for their accredited case management staff to approve/authorize inpatient encounters.

Note: We assume for purposes of this analysis that the health care provider is a hospital licensed under Article 28 of the New York Public Health Law.

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include: (1) the assignment of a unique identifier that is assigned in a confidential manner; and (2) certification in writing by the hospital and the user that the unique identifier is confidential and available only to the authorized user. *10 N.Y.C.R.R. § 405.10(c)(4)(i) and (ii)*.

Discussion

The requirement under New York law that hospitals assign each system user a unique identifier is consistent with HIPAA. See *45 C.F.R. § 164.312(a)(2)(i)*.

The assignment by the hospital of a unique user identifier to each of X Health Payer's case managers would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access. *10 N.Y.C.R.R. § 405.10(c)(4)(iv)*.

Hospitals must have procedures in place to modify or terminate use of an assigned identifier due to misuse or changes in the user's employment or affiliation with the hospital. *10 N.Y.C.R.R. § 405.10(c)(7)*.

Discussion

The requirement under New York law that hospitals have policies and procedures to restrict access to appropriately authorized individuals is consistent with HIPAA. See *45 C.F.R. §§ 164.308(a)(3)(i)(C), (4)(ii)(B) and (C)*. The requirement under New York law that hospitals adopt procedures to modify or terminate a system user's access rights based on the termination or modification of the user's relationship with the hospital is also consistent with HIPAA. See *45 C.F.R. § 164.308(a)(3)(ii)(C)*.

Assuming the patient has consented to grant the payer access to all his/her records for pre-authorization purposes, the hospital would appear to satisfy New York law if it adopts written policies and procedures (i) identifying and authenticating X Health Payer case management personnel who will have access to the EHR, (ii) requiring X Health Payer to monitor the scope of such access and promptly notify the hospital of abuse/misuse or the termination or reassignment of one of its case managers and (iii) obligating the hospital to terminate a case manager's access rights to the EHR upon notice from X Health Payer. Note: Hospitals currently do not afford open access rights to persons who are not their employees or who are not professionally affiliated (e.g. attending physicians, etc.) with the hospital. Rather, hospital staff provide the information to the case manager, rather than have the case manager be able to access any patient's record in the hospital, or even all (and not just the relevant parts) the record for their enrollees. Unless software was in place to restrict case managers only to their own enrollees and only to parts of the record for which reimbursement is pending or with respect to which some audit issue exists, it is unlikely that this arrangement would be determined to satisfy the security provisions of § 405.10.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 3

Domain Description

Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).*

Discussion

The general duty of hospitals to keep records confidential prohibits hospitals from releasing patient information to entities unless the patient and provider status can be verified. This is consistent with HIPAA which requires covered entities to verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information, if the identity or any such authority of such person is not known to the covered entity. *45 C.F.R. § 514(h).*

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 5

Domain Description

Information protections so that electronic personal health information cannot be improperly modified.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Hospitals are required to conduct audits to track access by system users. *10 N.Y.C.R.R. § 405.10(c)(4)(v)*. Public Health Law § 18(6) also requires the tracking and documentation by licensed professionals and facilities of certain disclosures to third parties (including initial disclosures to government and private payers). Either a copy of the subject's written authorization or the name of and address of such third party and a notation of the purpose of the disclosure must be indicated in the patient's file. Exceptions exist for facility staff and contractors, and government agencies for the purposes of facility inspections or professional conduct investigations.

Discussion

The requirement under *10 N.Y.C.R.R. § 405.10(c)(4)(v)* that hospitals conduct audits to track access by system users does not impose any specific obligations regarding the timing or nature of the mandated audits and is consistent with HIPAA. See *45 C.F.R. § 164.312(b)*. Periodic audits of the access to the hospital's records by other health care organizations would appear to satisfy New York law.

However, Public Health Law § 18(6) law requires additional tracking of disclosures by licensed professionals and facilities than is required under HIPAA. This provision requires tracking of disclosures made to external parties (including providers) not under contract with the disclosing provider, for initial payment disclosures to payers and for other disclosures not explicitly exempted in the law.

Key Legal Barriers

New York law requires additional administrative logging for disclosures by licensed providers beyond HIPAA mandates.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Hospitals must employ safeguards to ensure the security and confidentiality of their medical records. *10 N.Y.C.R.R. § 405.10(c)(4)*.

Hospitals must adopt policies and procedures to ensure the security of electronic or computer equipment from unwarranted access. *10 N.Y.C.R.R. § 405.10(c)(4)(iii)*.

Health care providers and health care facilities must adopt protocols for ensuring that records (including electronic records) containing HIV-related information are maintained securely and used for appropriate purposes. *10 N.Y.C.R.R. § 63.9(d)*.

Discussion

The requirement under New York that hospitals employ safeguards to ensure the confidentiality and security of their medical records is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. The same is true of the requirement under New York law that protocols be adopted to ensure records containing HIV-related information are securely maintained and appropriately used. The requirement under New York law that hospitals adopt policies and procedures to prevent

unwarranted access to computer equipment is consistent with HIPAA. See *45 C.F.R. § 164.310*.

The implementation of HIPAA-compliant safeguards, policies and procedures would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).* This regulation requires hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes. See also, *Williams v. Roosevelt Hospital, 66 N.Y.2d 391(1985)*. Physicians also are prohibited from disclosing identifiable information without consent, except if authorized or required by law. *Education Law §6530(23) and 8 N.Y.C.R.R. § 29.* Such state required consent may be a general consent permitting certain types of disclosures, and the consent does not have to be as specific as a HIPAA authorization or contain all of the HIPAA-mandated elements. If consent is oral or implied, it should be documented in the chart to enable enforcement and minimize litigation risk.

New York law contains a general requirement that disclosures by providers to third persons "shall be limited to that information necessary in light of the reason for disclosure." *New York Public Health Law § 18(6).* New York law also specifically addresses the scope of disclosures in limited circumstances, including disclosures related to HIV/AIDS, *New York Public Health Law § 2782* and mental health *New York Mental Hygiene Law §33.13.*

New York law permits medical services to be rendered without consent when in the physician's judgment an emergency exists and the person is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the person's life or health. *N.Y.P.H.L § 2504(4).* This provision has been interpreted to allow release of medical information under such circumstances, as well.

Health care providers may not disclose HIV-related information without the patient's authorization except for certain specifically defined purposes. *N.Y. Public Health Law Article 27-F*. In cases where the patient's authorization is required, the provider may not rely on a general consent; it must obtain a special HIV release that expressly references the nature of the information being disclosed and contains certain mandated elements. *N.Y. Public Health Law § 2780(9)*. The permitted purposes include disclosure to third party payers as necessary to obtain reimbursement for health care services, provided that, to the extent necessary under other laws, the provider or facility has obtained a general consent from the patient for the disclosure. *N.Y. Public Health Law § 2782(1)(i); 10 N.Y.C.R.R. § 63.6(a)(9)*. Disclosures to insurance institutions for reasons other than reimbursement are permitted only if the insurance institution obtains a written authorization stating the nature of the information being disclosed and the purpose of the disclosure. *N.Y. Public Health Law § 2782(1)(j); 10 N.Y.C.R.R. § 63.6(a)(10)*.

Hospitals operating mental health facilities licensed under Article 31 of the New York Mental Hygiene Law may disclose clinical records of such facilities without the patient's consent only for certain specifically defined purposes. Although the law does not expressly address the issue, the New York State Office of Mental Health ("OMH") is likely to take the position that mental health facilities may not rely on a general consent for the release of such records. OMH has developed a standard consent form for mental health facilities. The permitted purposes include disclosures to government agencies, licensed insurance companies and other third parties as necessary to obtain for reimbursement for mental health services. *N.Y. Mental Hygiene Law § 33.13(c)(9)(i)*.

Discussion

New York law is more stringent than HIPAA because it requires patient consent for the disclosure of protected health information by hospitals to health plans for reimbursement or other payment-related purposes. Such disclosures are permitted under HIPAA without patient consent or authorization. See *45 C.F.R. § 164.506(c)*.

At a minimum, New York law would require the hospital to obtain a general consent from each patient prior to permitting X Health Plan to have access to the patient's records. Most New York hospitals obtain a general consent from each patient as part of the admission or registration process. However, the language in the consent form may be narrowly tailored to permit the hospital to submit bills to the patient's insurer. A hospital would have to carefully review its consent form to determine whether the language is sufficiently broad to permit X Health Plan's access to the patient's entire EHR for pre-authorization purposes.

In addition, to the extent an EHR contains HIV-related information, it is unclear whether DOH would take the position that X Health Plan's access to the EHR for pre-authorization purposes falls within the reimbursement exception to New York's HIV confidentiality law. There appears to be a strong argument that it does because pre-authorization is a condition of payment. However, if the law were interpreted more restrictively, the hospital or payer would have to obtain a more specific authorization from any patient whose EHR contained HIV-related information.

Likewise, to the extent an EHR is maintained by a hospital facility licensed under Article 31 of the Mental Hygiene Law, it is unclear whether OMH would take the position that X Health Plan's access to the EHR for pre-authorization purposes falls within the reimbursement exception to New York's mental health confidentiality law. There appears to be a strong argument that it does because pre-authorization is a condition of payment. However, if the law were interpreted more restrictively, the hospital would have to obtain a more specific patient consent prior to providing access to its mental health facility records.

New York law's general requirement that all disclosures by providers to third persons are limited to that information necessary in light of the reason for disclosure exceed the HIPAA concept of "minimum necessary," which does not apply to release of information for treatment purposes. However, here, where the disclosure is for payment purposes, New York law would not exceed HIPAA requirements.

Key Legal Barriers

The hospital or payer might have to revise its standard consent form to cover the provision of access to the EHR to X Health Plan. In addition, depending on how New York's HIV and mental health confidentiality laws are interpreted by DOH and OMH, respectively, the hospital or payer might be required to obtain a more specific patient authorization covering HIV and mental health records, which would effectively preclude X Health Plan from gaining access to this information.

6. RHIO Scenario

The RHIO in your region wants to access patient identifiable data from all participating organizations (and their patients) to monitor the incidence and management of diabetic patients. The RHIO also intends to monitor participating providers to rank them for the provision of preventive services to their diabetic patients.

Note: We assume for purposes of this analysis that the RHIO consists of hospitals, private physician practices, pharmacies and clinical laboratories. We also assume that the data regarding diabetic patients does not include HIV-related or mental health information

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include: (1) the assignment of a unique identifier that is assigned in a confidential manner; and (2) certification in writing by the hospital and the user that the unique identifier is confidential and available only to the authorized user. *10 N.Y.C.R.R. § 405.10(c)(4)(i) and (ii)*.

Discussion

The requirement under New York law that hospitals assign each system user a unique identifier is consistent with HIPAA. See *45 C.F.R. § 164.312(a)(2)(i)*.

The assignment of a unique user identifier to each RHIO employee accessing hospital data would appear to satisfy New York law. However, the monitoring and enforcement of the consistent use of the identifier by the same non-hospital based employee must be assured.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access. *10 N.Y.C.R.R. § 405.10(c)(4)(iv)*.

Hospitals must have procedures in place to modify or terminate use of an assigned identifier due to misuse or changes in the user's employment or affiliation with the hospital. *10 N.Y.C.R.R. § 405.10(c)(7)*.

Only pharmacists and pharmacy interns may "access the data" in a computerized prescription management system maintained by a pharmacy, except that unlicensed persons may be granted such access to assist with specified administrative functions. *8 N.Y.C.R.R. §§ 29.7(a)(8)(vii) and (a)(21)*. The phrase "access the data" is not defined in the regulations.

Discussion

The requirement under New York law that hospitals have policies and procedures to restrict access to appropriately authorized individuals is consistent with HIPAA. See *45 C.F.R. §§ 164.308(a)(3)(i)(C), (4)(ii)(B) and (C)*. The requirement under New York law that hospitals adopt procedures to modify or terminate a system user's access rights based on the termination or modification of the user's relationship with the hospital is also consistent with HIPAA. See *45 C.F.R. § 164.308(a)(3)(ii)(C)*. The hospitals would appear to satisfy New York law if they adopt written policies and procedures (i) identifying RHIO personnel who will have access to their records, (ii) requiring the RHIO to monitor such access and to promptly notify the hospital of the termination or reassignment of one of these employees and (iii) obligating the hospital to terminate a RHIO employee's access rights to the system upon notice from the RHIO.

Although New York regulations state that pharmacies must restrict access to licensed professionals or other pharmacy personnel performing administrative functions, it is not clear how "access the data" is defined in this context. If "access the data" does not include accessing patient identifiable data that is extracted from the original prescription record in the electronic data processing system, the pharmacies could provide access to the RHIO without violating the above-cited regulation. However, if "access the data" means the capacity to receive the patient information in the data, the above-cited regulation might be construed as prohibiting the RHIO from accessing the information in the pharmacies' electronic prescription management system. Such an interpretation would make New York law more stringent than HIPAA, which permits the pharmacies to share data with the RHIO for quality improvement purposes if the RHIO is functioning as the pharmacies' business associate. *45 C.F.R. §§ 164.502(e), 504(e) and 164.506(c)*.

Key Legal Barriers

If New York law is interpreted as prohibiting pharmacies from permitting individuals other than pharmacists, pharmacy interns or their administrative personnel from viewing data in a pharmacy's prescription data management system, this would prohibit the RHIO from directly accessing data in pharmacies' information systems.

Domain 3

Domain Description

Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).*

Discussion

The general duty of hospitals to keep records confidential prohibits hospitals from releasing patient information to entities unless the patient and provider status can be verified. This is consistent with HIPAA which requires covered entities to verify the identity of a person requesting protected health information and the authority of any such person to have access

to protected health information, if the identity or any such authority of such person is not known to the covered entity. *45 C.F.R. § 514(h).*

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 5

Domain Description

Information protections so that electronic personal health information cannot be improperly modified.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Pharmacies utilizing a computerized prescription management system "shall provide adequate safeguards against improper manipulation or alteration of stored records." *8 N.Y.C.R.R. § 29.7(a)(8)(i)*.

Discussion

The requirement that hospitals employ safeguards to ensure safety nd confidentiality under New York law is general in nature and does not exceed HIPAA requirements.

The requirement that pharmacies adopt safeguards against improper manipulation or alteration of stored records parallels the obligation of covered entities under HIPAA to implement integrity controls. 45 C.F.R. § 164.312(c). Compliance with this HIPAA mandate would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Hospitals are required to conduct audits to track access by system users. *10 N.Y.C.R.R. § 405.10(c)(4)(v)*. Public Health Law § 18(6) also requires the tracking and documentation by licensed professionals and facilities of certain disclosures to third parties (including initial disclosures to government and private payers). Either a copy of the subject's written authorization or the name of and address of such third party and a notation of the purpose of the disclosure must be indicated in the patient's file. Exceptions exist for facility staff and contractors, and government agencies for the purposes of facility inspections or professional conduct investigations.

Discussion

The requirement under *10 N.Y.C.R.R. § 405.10(c)(4)(v)* that hospitals conduct audits to track access by system users does not impose any specific obligations regarding the timing or nature of the mandated audits and is consistent with HIPAA. See *45 C.F.R. § 164.312(b)*. Periodic audits of the access to the hospital's records by other health care organizations would appear to satisfy New York law.

However, Public Health Law § 18(6) law requires additional tracking of disclosures by licensed professionals and facilities than is required under HIPAA. This provision requires tracking of disclosures made to external parties (including providers) not under contract with the disclosing provider, for initial payment disclosures to payers and for other disclosures not explicitly exempted in the law.

Key Legal Barriers

New York law requires additional administrative logging for disclosures by licensed providers beyond HIPAA mandates.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Hospitals must employ safeguards to ensure the security and confidentiality of their medical records. *10 N.Y.C.R.R. § 405.10(c)(4)*.

Hospitals must adopt policies and procedures to ensure the security of electronic or computer equipment from unwarranted access. *10 N.Y.C.R.R. § 405.10(c)(4)(iii)*.

Discussion

The requirement under New York that hospitals employ safeguards to ensure the confidentiality and security of their medical records is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. The requirement under New York law that hospitals adopt policies and procedures to prevent unwarranted access to computer equipment is consistent with HIPAA. See *45 C.F.R. § 164.310*.

The implementation of HIPAA-compliant safeguards, policies and procedures by the hospitals would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).* This regulation requires hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes. See also, *Williams v. Roosevelt Hospital, 66 N.Y.2d 391(1985)*. Physicians also are prohibited from disclosing identifiable information without consent, except if authorized or required by law. *Education Law §6530(23) and 8 N.Y.C.R.R. § 29.* Such state required consent may be a general consent permitting certain types of disclosures, and the consent does not have to be as specific as a HIPAA authorization or contain all of the HIPAA-mandated elements. If consent is oral or implied, it should be documented in the chart to enable enforcement and minimize litigation risk.

New York law permits medical services to be rendered without consent when in the physician's judgment an emergency exists and the person is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the person's life or health. *N.Y.P.H.L § 2504(4).* This provision has been interpreted to allow release of medical information under such circumstances, as well.

It is professional misconduct for pharmacists and physicians to reveal "personally identifiable facts, data or information obtained in a professional capacity without the prior consent of the patient or client, except as authorized or required by law." *N.Y. Education Law § 6530(23);* 8 N.Y.C.R.R. § 29.1(b)(8). DOH has interpreted this regulation in a manner similar to its interpretation of the above-cited hospital regulation, i.e., pharmacists and physicians are required to obtain patient consent for the disclosure of records to outside entities, even for treatment, quality improvement or other purposes permitted by HIPAA without patient authorization.

Clinical laboratories may report test results only to "a physician, his agent, or other person authorized by law to employ the results thereof in the conduct of his practice or in the fulfillment of his official duties." *10 N.Y.C.R.R. § 58-1.8*. It is unclear how the term "agent" is defined under this regulation and whether the RHIO could serve as the physician's agent if the

physician authorized the RHIO, in a written agreement or otherwise, to receive test results on his or her behalf.

Discussion

New York law is more stringent than HIPAA because it requires patient consent for the disclosure of protected health information by hospitals, physicians and pharmacists to an outside entity such as the RHIO for quality improvement purposes. Such disclosures are permitted under HIPAA without patient consent or authorization. See *45 C.F.R. § 164.506(c)(4)*. Data aggregation also is permitted by business associates under HIPAA. 45 C.F.R. §§ 164.501, 164.504(e)(2)(i)(B).

New York law would require the hospitals, pharmacies and physicians participating in the RHIO to obtain a general consent from each patient prior to permitting the RHIO to have access to the patient's records. Most New York hospitals and some physicians obtain a general consent from each patient as part of the admission or registration process. However, the language in the consent form may be narrowly tailored to permit the hospital or physician to provide treatment or submit bills to the patient's insurer. Hospitals and physicians would have to carefully review their consent forms to determine whether the language is sufficiently broad to permit the RHIO to obtain access to their patients' records. In addition, pharmacies typically do not obtain patient consents as part of their standard business practices.

Clinical laboratories would not be permitted to send test results to the RHIO under New York law unless the RHIO were deemed the physician's "agent" under the clinical laboratory regulation cited above. Clarification would be required from DOH to determine how the term "agent" is defined in this context. If test results could not be transmitted by the clinical laboratories, it might be possible for the RHIO to obtain the results from the ordering physician if the physician obtained patient consent as described above.

Key Legal Barriers

The hospitals and physicians might have to revise their standard consent forms to cover the disclosure of information to the RHIO.

The pharmacies would not be permitted to share information with the RHIO unless they obtained patient consents, which would constitute a new business practice that is unlikely to be adopted by most pharmacies.

The clinical laboratories would be permitted to share information with the RHIO only if they could be deemed the ordering physician's agent under applicable regulations.

7. Research Data Use Scenario

A research project on children younger than age 13 is being conducted in a double blind study for a new drug for ADD/ADHD. The research is being sponsored by a major drug manufacturer conducting a double blind study approved by the medical center's IRB where the research investigators are located. The data being collected is all electronic and all responses from the subjects are completed electronically on the same centralized and shared data base file. The principle investigator was asked by one of the investigators if they could use the raw data to extend the tracking of the patients over an additional six months and/or use the raw data collected for a white paper that is not part of the research protocols final document for his post doctoral fellow program.

Note: We assume for purposes of this analysis that the medical center is a hospital licensed under Article 28 of the New York Public Health Law.

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include: (1) the assignment of a unique identifier that is assigned in a confidential manner; and (2) certification in writing by the hospital and the user that the unique identifier is confidential and available only to the authorized user. *10 N.Y.C.R.R. § 405.10(c)(4)(i) and (ii)*.

Discussion

The requirement under New York law that hospitals assign each system user a unique identifier is consistent with HIPAA. See *45 C.F.R. § 164.312(a)(2)(i)*.

The assignment by the hospital of a unique user identifier to each investigator would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access. *10 N.Y.C.R.R. § 405.10(c)(4)(iv)*.

Hospitals must have procedures in place to modify or terminate use of an assigned identifier due to misuse or changes in the user's employment or affiliation with the hospital. *10 N.Y.C.R.R. § 405.10(c)(7)*.

Discussion

The requirement under New York law that hospitals have policies and procedures to restrict access to appropriately authorized individuals is consistent with HIPAA. See *45 C.F.R. §§ 164.308(a)(3)(i)(C), (4)(ii)(B) and (C)*. The requirement under New York law that hospitals adopt procedures to modify or terminate a system user's access rights based on the termination or modification of the user's relationship with the hospital is also consistent with HIPAA. See *45 C.F.R. § 164.308(a)(3)(ii)(C)*.

The hospital would appear to satisfy New York law if it adopts written policies and procedures identifying the researchers who have access to the hospital's medical records, specifying the nature of their access and providing for the termination of their access rights under appropriate circumstances.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 3

Domain Description

Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).*

Discussion

The general duty of hospitals to keep records confidential prohibits hospitals from releasing patient information to entities unless the patient and provider status can be verified. This is consistent with HIPAA which requires covered entities to verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information, if the identity or any such authority of such person is not known to the covered entity. *45 C.F.R. § 514(h).*

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 5

Domain Description

Information protections so that electronic personal health information cannot be improperly modified.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Hospitals are required to conduct audits to track access by system users. *10 N.Y.C.R.R. § 405.10(c)(4)(v)*. Public Health Law § 18(6) also requires the tracking and documentation by licensed professionals and facilities of certain disclosures to third parties (including initial disclosures to government and private payers). Either a copy of the subject's written authorization or the name of and address of such third party and a notation of the purpose of the disclosure must be indicated in the patient's file. Exceptions exist for facility staff and contractors, and government agencies for the purposes of facility inspections or professional conduct investigations.

Discussion

The requirement under *10 N.Y.C.R.R. § 405.10(c)(4)(v)* that hospitals conduct audits to track access by system users does not impose any specific obligations regarding the timing or

nature of the mandated audits and is consistent with HIPAA. See *45 C.F.R. § 164.312(b).* Periodic audits of the access to the hospital's records by other health care organizations would appear to satisfy New York law.

However, Public Health Law § 18(6) law requires additional tracking of disclosures by licensed professionals and facilities than is required under HIPAA. This provision requires tracking of disclosures made to external parties (including providers) not under contract with the disclosing provider, for initial payment disclosures to payers and for other disclosures not explicitly exempted in the law.

Key Legal Barriers

New York law requires additional administrative logging for disclosures by licensed providers beyond HIPAA mandates.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Hospitals must employ safeguards to ensure the security and confidentiality of their medical records. *10 N.Y.C.R.R. § 405.10(c)(4)*.

Hospitals must adopt policies and procedures to ensure the security of electronic or computer equipment from unwarranted access. *10 N.Y.C.R.R. § 405.10(c)(4)(iii)*.

Discussion

The requirement under New York that hospitals employ safeguards to ensure the confidentiality and security of their medical records is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. The requirement under New York law that hospitals adopt policies and procedures to prevent unwarranted access to computer equipment is consistent with HIPAA. See *45 C.F.R. § 164.310*.

The implementation of HIPAA-compliant safeguards, policies and procedures would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).* This regulation requires hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes. See also, *Williams v. Roosevelt Hospital, 66 N.Y.2d 391(1985)*. Physicians also are prohibited from disclosing identifiable information without consent, except if authorized or required by law. *Education Law §6530(23) and 8 N.Y.C.R.R. § 29.* Such state required consent may be a general consent permitting certain types of disclosures, and the consent does not have to be as specific as a HIPAA authorization or contain all of the HIPAA-mandated elements. If consent is oral or implied, it should be documented in the chart to enable enforcement and minimize litigation risk.

New York law permits medical services to be rendered without consent when in the physician's judgment an emergency exists and the person is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the person's life or health. *N.Y.P.H.L § 2504(4).* This provision has been interpreted to allow release of medical information under such circumstances, as well.
The New York Law for the protection of human research subjects is not applicable to research "which is subject to, and which is in compliance with, [federal] policies and regulations." *N.Y. Public Health Law § 2445*. Thus, DOH has interpreted this law not to apply to: (a) federally-funded research reviewed by an IRB registered with the federal Office for Human Research Protections (OHRP) pursuant to a Federalwide Assurance (FWA); or (b) non-federally-funded research reviewed by an IRB registered with OHRP pursuant to a FWA under which the institution conducting the research has agreed that its activities related to human subject research, regardless of funding source, will be guided by the Belmont Report and carried out in compliance with 45 CFR Part 46; or (c) clinical investigations for products as part of the process for obtaining Food and Drug Administration (FDA) approval that are carried out in compliance with all applicable federal FDA laws, regulations and rules.

In the rare instances when the law is applicable for research on human subjects, New York requires that each person participating in research (or, if the person is a minor, the minor's parent or legal guardian) consent in writing to the research. *N.Y. Public Health Law § 2442.* "Human research" "involves physical or psychological intervention by the researcher upon the body of the subject," and does not include "epidemiological investigations." *N.Y. Public Health Law § 2441(2).* The basic information necessary to any consent for research includes a "fair explanation" of the "procedure to be followed, and their purposes, including identification of any procedures which are experimental." *N.Y. Public Health Law § 2441(5)(a)*. New York does not have any statutes or regulations that address the disclosure of information obtained in connection with research in this context.

Discussion

Most New York hospitals obtain a general consent from each patient as part of the admission or registration process, and in the case of research, the hospital must obtain a voluntary informed consent. The medical center would need to evaluate whether the language in these consents is broad enough to encompass giving access to the investigator to use the data for research outside the scope of the study approved by the medical center's IRB. It is unlikely that either consent would allow for the access and use the investigator is seeking. If the medical center wants to allow the investigator to use the data, it could try to obtain the consent to do so from the patient's parent or legal guardian and the assent of the child. The medical center could also ask the IRB to waive the requirement to get informed consent for human subject research and to waive the requirement to get an authorization under HIPAA. See *45 C.F.R. §§ 46.116(d); 164.512(i)(1)(i).* However, it is doubtful that the criteria for granting those waivers could be satisfied, and it is unclear if a waiver of authorization would

be an acceptable substitute for patient consent under New York law since New York law is silent on this issue.

Key Legal Barriers

If the medical center wanted to allow further research by the investigator, it would need to either obtain consent from the patient or obtain a waiver of authorization from the IRB, and it is possible that the latter option would not be possible under federal law and would not satisfy New York law.

8. Scenario for access by law enforcement

An injured nineteen (19) year old college student is brought to the ER following an automobile accident. It is standard to run blood alcohol and drug screens. The police officer investigating the accident arrives in the ER claiming that the patient may have caused the accident. The patient's parents arrive shortly afterward. The police officer requests a copy of the blood alcohol test results and the parents want to review the ER record and lab results to see if their child tested positive for drugs. These requests to print directly from the electronic health record are made to the ER staff. The patient is covered under their parent's health and auto insurance policy.

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include: (1) the assignment of a unique identifier that is assigned in a confidential manner; and (2) certification in writing by the hospital and the user that the unique identifier is confidential and available only to the authorized user. *10 N.Y.C.R.R. § 405.10(c)(4)(i) and (ii)*.

Discussion

The requirement under New York law that hospitals assign each system user a unique identifier is consistent with HIPAA. See *45 C.F.R. § 164.312(a)(2)(i)*.

The assignment by the hospital of a unique user identifier to any person permitted access to its records would appear to satisfy New York law. This is likely irrelevant in this scenario, though, because the hospital would probably not allow a parent or police officer access to its records.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access. *10 N.Y.C.R.R. § 405.10(c)(4)(iv)*.

Hospitals must have procedures in place to modify or terminate use of an assigned identifier due to misuse or changes in the user's employment or affiliation with the hospital. *10 N.Y.C.R.R. § 405.10(c)(7)*.

Discussion

The requirement under New York law that hospitals have policies and procedures to restrict access to appropriately authorized individuals is consistent with HIPAA. See *45 C.F.R. §§ 164.308(a)(3)(i)(C), (4)(ii)(B) and (C)*. The requirement under New York law that hospitals adopt procedures to modify or terminate a system user's access rights based on the termination or modification of the user's relationship with the hospital is also consistent with HIPAA. See *45 C.F.R. § 164.308(a)(3)(ii)(C)*.

The hospital would appear to satisfy New York law if it adopts written policies and procedures identifying any persons that have access to the hospital's medical records and the nature of their access and terminating their access rights under appropriate circumstances. This likely irrelevant in this scenario, though, because the hospital would probably not allow a parent or police officer access to its records.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 3

Domain Description

Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).*

Discussion

The general duty of hospitals to keep records confidential prohibits hospitals from releasing patient information to entities unless the patient and provider status can be verified. This is consistent with HIPAA which requires covered entities to verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information, if the identity or any such authority of such person is not known to the covered entity. *45 C.F.R. § 514(h).*

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 5

Domain Description

Information protections so that electronic personal health information cannot be improperly modified.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Hospitals are required to conduct audits to track access by system users. *10 N.Y.C.R.R. § 405.10(c)(4)(v)*. Public Health Law § 18(6) also requires the tracking and documentation by licensed professionals and facilities of certain disclosures to third parties (including initial disclosures to government and private payers). Either a copy of the subject's written

authorization or the name of and address of such third party and a notation of the purpose of the disclosure must be indicated in the patient's file. Exceptions exist for facility staff and contractors, and government agencies for the purposes of facility inspections or professional conduct investigations.

Discussion

The requirement under *10 N.Y.C.R.R. § 405.10(c)(4)(v)* that hospitals conduct audits to track access by system users does not impose any specific obligations regarding the timing or nature of the mandated audits and is consistent with HIPAA. See *45 C.F.R. § 164.312(b).* Periodic audits of the access to the hospital's records by other health care organizations would appear to satisfy New York law.

However, Public Health Law § 18(6) law requires additional tracking of disclosures by licensed professionals and facilities than is required under HIPAA. This provision requires tracking of disclosures made to external parties (including providers) not under contract with the disclosing provider, for initial payment disclosures to payers and for other disclosures not explicitly exempted in the law.

Key Legal Barriers

New York law requires additional administrative logging for disclosures by licensed providers beyond HIPAA mandates.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Hospitals must employ safeguards to ensure the security and confidentiality of their medical records. *10 N.Y.C.R.R. § 405.10(c)(4)*.

Hospitals must adopt policies and procedures to ensure the security of electronic or computer equipment from unwarranted access. *10 N.Y.C.R.R. § 405.10(c)(4)(iii)*.

Discussion

The requirement under New York that hospitals employ safeguards to ensure the confidentiality and security of their medical records is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. The requirement under New York law that hospitals adopt policies and procedures to prevent unwarranted access to computer equipment is consistent with HIPAA. See *45 C.F.R. § 164.310*.

The implementation of HIPAA-compliant safeguards, policies and procedures would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond the requirements of HIPAA.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).* This regulation requires hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes. See also, *Williams v. Roosevelt Hospital, 66 N.Y.2d 391(1985)*. Physicians also are prohibited from disclosing identifiable information without consent, except if authorized or required by law. *Education Law §6530(23) and 8 N.Y.C.R.R. § 29.* Such state required consent may be a general consent permitting certain types of disclosures, and the consent does not have to be as specific as a HIPAA authorization or contain all of the HIPAA-mandated elements. If consent is oral or implied, it should be documented in the chart to enable enforcement and minimize litigation risk.

New York law permits medical services to be rendered without consent when in the physician's judgment an emergency exists and the person is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the person's life or health. *N.Y.P.H.L § 2504(4).* This provision has been interpreted to allow release of medical information under such circumstances, as well.

A minor in New York is defined as a person less than 18 years of age. *See N.Y. General Obligations Law § 1-202, N.Y. Domestic Relations Law § 2 and N.Y. Public Health Law § 2504.*

In the motor vehicle situation, NYS Vehicle and Traffic Law § 1194 states : "Any person who operates a motor vehicle in this state shall be deemed to have given consent to a chemical test of one or more of the following: breath, blood, urine, or saliva, for the purpose of determining the alcoholic and/or drug content of the blood provided that such test is administered by or at the direction of a police officer…." 10 N.Y.C.R.R. § 58-1.7 permits police to submit samples to a laboratory and 10 N.Y.C.R.R. §58-1.8 permits labs to disclose results to persons when in the fulfillment of their official duties.

Discussion

New York law would require consent for release of the ER record and lab results to the parents. Since the patient is 19 years old, s/he is of majority age in New York and his/her parents do not possess any special status with respect to his/her medical records. An example of an exception to this would be if his/her parents were his/her guardian due to due to mental disability, but a competent 19 year-old is an adult in New York.

Most New York hospitals obtain a general consent from each patient as part of the admission or registration process so it is possible the hospital already has what it needs, but the language in the consent form may be narrowly tailored to permit the hospital to submit bills to the patient's insurer. The hospital would have to carefully review its consent form to determine whether the language is sufficiently broad to permit the disclosures requested here.

New York law would not require the patient's consent for release of the blood alcohol tests results to the police. Under the New York State Vehicle and Traffic Law, the patient would be deemed to have given consent for a test taken at the direction of a police officer. Thus, the hospital could fulfill the police request for access to the blood alcohol test records without further consent.

New York law is less restrictive than HIPAA in this area. HIPAA provides exceptions for when disclosure of information in medical records can be made without the patient's consent. *See 45 C.F.R. § 164.512*. HIPAA exceptions for law enforcement purposes generally would not allow disclosure to the police officer without patient consent or a subpoena unless otherwise required by law. *See 45 C.F.R. § 164.512(f).*

Key Legal Barriers

New York law does not create a barrier to release of information to police. New York law protects the confidentiality of patient records in ways that create barriers to release to parents.

9. Pharmacy Benefit A Scenario

The Pharmacy Benefit Manager (PBM) has a mail order pharmacy for a hospital which is self-insured and also has a closed formulary. The PBM receives a prescription from Patient X, an employee of the hospital, for the antipsychotic medication Geodon. The PBM's preferred alternatives for antipsychotics are Risperidone (Risperdal), Quetiapine (Seroquel), and Aripiprazole (Abilify). Since Geodon is not on the preferred alternatives list, the PBM sends a request to the prescribing physician to complete a prior authorization in order to fill and pay for the Geodon prescription. The PBM is in a different state than the provider's Outpatient Clinic.

Note: New York does not directly regulate the operations of PBMs. Given the fact that the hospital's health benefit plan is self-insured, New York legal requirements governing state-licensed health plans are not applicable to the PBM in this scenario. Therefore, we analyze this scenario solely under New York laws governing pharmacies. We assume for purposes of this analysis that the mail order pharmacy is located in or otherwise subject to the laws of New York State. Out-of-state mail order pharmacies are generally subject to the New York regulatory requirements referenced below. See *8 N.Y.C.R.R. §§ 29.7(c) and 63.8*.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

Only pharmacists and pharmacy interns may access data in a computerized prescription management system maintained by a pharmacy, except that unlicensed persons may be granted such access to assist with specified administrative functions. *8 N.Y.C.R.R. §§ 29.7(a)(8)(vii) and (a)(21)*.

Discussion

The requirement under New York law that pharmacies restrict access to licensed professionals or other pharmacy personnel performing administrative functions is consistent with HIPAA's minimum necessary and role-based access requirements. See *45 C.F.R. §§ 164.514(d)(2) and 164.308(a)(4)(ii)(B) and (C)*. The pharmacy would not be required to take additional steps to comply with New York law if it had adopted role-based access policies and procedures required by HIPAA.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 5

Domain Description

Information protections so that electronic personal health information cannot be improperly modified.

Applicable New York Law

Pharmacies utilizing a computerized prescription management system "shall provide adequate safeguards against improper manipulation or alteration of stored records." *8 N.Y.C.R.R. § 29.7(a)(8)(i)*.

Discussion

The requirement under New York law that a pharmacy employ adequate safeguards against improper manipulation or alteration of stored records parallels the obligation of covered entities under HIPAA to implement integrity controls. *45 C.F.R. § 164.312(c)*. Compliance with this HIPAA mandate would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Public Health Law § 18(6) requires the tracking and documentation by licensed professionals of certain disclosures to third parties (including initial disclosures to government and private payers). Either a copy of the subject's written authorization or the name of and address of such third party and a notation of the purpose of the disclosure must be indicated in the patient's file. Exceptions exist for facility staff and contractors, and government agencies for the purposes of facility inspections or professional conduct investigations.

Discussion

Public Health Law § 18(6) law requires additional tracking of disclosures by licensed professionals than is required under HIPAA. This provision requires tracking of disclosures made to external parties (including providers) not under contract with the disclosing provider, for initial payment disclosures to payers and for other disclosures not explicitly exempted in the law.

Key Legal Barriers

New York law requires additional administrative logging for disclosures by licensed providers beyond HIPAA mandates.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

It is professional misconduct for a pharmacist to reveal "personally identifiable facts, data or information obtained in a professional capacity without the prior consent of the patient or client, except as authorized or required by law." 8 N.Y.C.R.R. § 29.1(b)(8). A similar law applicable to physicians has been interpreted by DOH as requiring patient consent for disclosures of patient information to outside entities, even for payment purposes. *N.Y. Education Law § 6530(23).* However, there appears to be a reasonable argument that a prior authorization request submitted by a pharmacist to a prescribing physician does not constitute

the "revealing of personally identifiable information" because the prescribing physician already has, and, in fact, is the source of, the information being conveyed by the pharmacist. Indeed, it is common practice for New York pharmacies (including mail order pharmacies) to make such communications to prescribing physicians without patient consent and no regulatory authority has suggested this conduct is improper. Therefore, it appears that such communications are not deemed inconsistent with the above-cited regulation.

Discussion

To the extent the above-cited regulation is interpreted to require patient consent for a pharmacy to make a pre-authorization request to a prescribing physician, New York law is more stringent than HIPAA because it requires patient consent for the disclosure of protected health information for payment-related purposes. Such disclosures are permitted under HIPAA without patient consent or authorization. See *45 C.F.R. § 164.506(c)*. However, as indicated above, it does not appear that New York has interpreted the regulation as requiring patient consent for such purposes. Therefore, New York law appears to be consistent with HIPAA.

Key Legal Barriers

Although there do not appear to be any clear legal barriers, it would be helpful if the Pharmacy Board or other New York regulatory authorities clarified that the above-cited regulation does not require pharmacists to obtain patient consent to make prior authorization requests to prescribing physician.

11. Healthcare Operations and Marketing – Scenario A

ABC Health Care is an integrated health delivery system comprised of ten critical access hospitals and one large tertiary hospital, DEF Medical Center, which has served as the system's primary referral center. Recently, DEF Medical Center has expanded its rehab services and created a state-of-the-art, stand-alone rehab center. Six months into operation, ABC Health Care does not feel that the rehab center is being fully utilized and is questioning the lack of rehab referrals from the critical access hospitals.

ABC Health Care has requested that its critical access hospitals submit monthly reports containing patient identifiable data to the system six-sigma team to analyze patient encounters and trends for the following rehab diagnoses/ procedures:

- Cerebrovascular Accident (CVA)
- Hip Fracture
- Total Joint Replacement

Additionally, ABC Health Care is requesting that this same information, along with individual patient demographic information, be provided to the system Marketing Department. The Marketing Department plans to distribute to these individuals a brochure highlighting the new rehab center and the enhanced services available.

Note: We assume for purposes of analyzing this scenario that DEF Medical Center and the ten critical access hospitals are all separate not-for-profit entities under the common control of another not-for-profit organization ("ABC Parent"). We also assume that the individuals working in the Marketing Department are employees of ABC Parent. In addition, we assume that the critical access hospitals, DEF Medical Center and ABC Parent share an electronic information system managed by ABC Parent.

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include: (1) the assignment of a unique identifier that is assigned in a confidential manner; and (2) certification in writing by the hospital and the user that the unique identifier is confidential and available only to the authorized user. *10 N.Y.C.R.R. § 405.10(c)(4(i) and (ii)*.

Discussion

The requirement under New York law that hospitals assign each system user a unique identifier is consistent with HIPAA. See *45 C.F.R. § 164.312(a)(2)(i)*.

The assignment by ABC Parent of a unique user identifier to each employee of ABC Parent and DEF Medical Center accessing data transmitted by the critical access hospitals would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

Hospitals are required to employ safeguards to ensure the security and confidentiality of their medical records. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access. *10 N.Y.C.R.R. § 405.10(c)(4)(iv)*.

Hospitals must have procedures in place to modify or terminate use of an assigned identifier due to misuse or changes in the user's employment or affiliation with the hospital. *10 N.Y.C.R.R. § 405.10(c)(7)*.

Discussion

The requirement under New York law that hospitals have policies and procedures to restrict access to appropriately authorized individuals is consistent with HIPAA. See *45 C.F.R. §§ 164.308(a)(3)(i)(C), (4)(ii)(B) and (C)*. The requirement under New York law that hospitals adopt procedures to modify or terminate a system user's access rights based on the termination or modification of the user's relationship with the hospital is also consistent with HIPAA. See *45 C.F.R. § 164.308(a)(3)(ii)(C)*.

The critical access hospitals would appear to satisfy New York law if they adopt written policies and procedures (i) identifying the types of ABC Parent and DEF Medical Center personnel who will have access to their data, (ii) requiring DEF Medical Center to promptly notify ABC Parent of the termination or reassignment of one of DEF Medical Center's employees and (iii) obligating ABC Parent to terminate an ABC Parent or DEF Medical Center employee's access rights to the critical access hospitals' data upon termination or reassignment.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 3

Domain Description

Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).*

Discussion

The general duty of hospitals to keep records confidential prohibits hospitals from releasing patient information to entities unless the patient and provider status can be verified. This is consistent with HIPAA which requires covered entities to verify the identity of a person

requesting protected health information and the authority of any such person to have access to protected health information, if the identity or any such authority of such person is not known to the covered entity. *45 C.F.R. § 514(h).*

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 5

Domain Description

Information protections so that electronic personal health information cannot be improperly modified.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Hospitals are required to conduct audits to track access by system users. *10 N.Y.C.R.R. § 405.10(c)(4)(v)*. Public Health Law § 18(6) also requires the tracking and documentation by licensed professionals and facilities of certain disclosures to third parties (including initial disclosures to government and private payers). Either a copy of the subject's written authorization or the name of and address of such third party and a notation of the purpose of the disclosure must be indicated in the patient's file. Exceptions exist for facility staff and contractors, and government agencies for the purposes of facility inspections or professional conduct investigations.

Discussion

The requirement under *10 N.Y.C.R.R. § 405.10(c)(4)(v)* that hospitals conduct audits to track access by system users does not impose any specific obligations regarding the timing or nature of the mandated audits and is consistent with HIPAA. See *45 C.F.R. § 164.312(b).* Periodic audits by the critical access hospitals (or by ABC Parent on their behalf) of the use of data by the hospitals' employees and the access to data DEF Medical Center and ABC Parent employees would appear to satisfy New York law.

If DEF Medical Center and ABC Parent have a contractual relationship, it would fall within the exceptions under Public Health Law § 18(6), and therefore, would not be subject to additional tracking of disclosures.

Key Legal Barriers

Assuming DEF Medical Center and ABC Parent have a contractual relationship, New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Hospitals must employ safeguards to ensure the security and confidentiality of their medical records. *10 N.Y.C.R.R. § 405.10(c)(4)*.

Hospitals must adopt policies and procedures to ensure the security of electronic or computer equipment from unwarranted access. *10 N.Y.C.R.R. § 405.10(c)(4)(iii)*.

Discussion

The requirement under New York that hospitals employ safeguards to ensure the confidentiality and security of their medical records is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. The requirement under New York law that hospitals adopt policies and procedures to prevent

unwarranted access to computer equipment is consistent with HIPAA. See *45 C.F.R. § 164.310*.
The implementation of HIPAA-compliant safeguards, policies and procedures would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).* This regulation requires hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes. See also, *Williams v. Roosevelt Hospital, 66 N.Y.2d 391(1985)*. Physicians also are prohibited from disclosing identifiable information without consent, except if authorized or required by law. *Education Law §6530(23) and 8 N.Y.C.R.R. § 29.* Such state required consent may be a general consent permitting certain types of disclosures, and the consent does not have to be as specific as a HIPAA authorization or contain all of the HIPAA-mandated elements. If consent is oral or implied, it should be documented in the chart to enable enforcement and minimize litigation risk.

Although we are unaware of any formal interpretation of the term "disclosure" by DOH, it does not appear that DOH construes the term to include internal uses of information within a hospital. It is unclear, though, how DOH might apply the above-cited regulation to the exchange of patient data among affiliated hospitals, or between a hospital and its parent company, and whether such exchanges would be considered "disclosures" triggering the patient consent requirement. If hospitals are separately established, they are independently responsible for maintaining the confidentiality of identifiable medical information within that hospital. Disclosures outside the facility must be consented or fall into one of the exceptions, e.g. the institution is clinically integrated into a larger network, such that the network does quality assurance.

Discussion

The HIPAA analysis of this scenario appears to hinge on whether the critical access hospitals, DEF Medical Center and ABC Parent are part of a single covered entity for HIPAA compliance purposes. If they are part of a single covered entity, the exchange of information contemplated by this scenario would appear to qualify as "business planning and development," which falls within the definition of health care operations. *45 C.F.R. §§ 164.501*. A covered entity may internally use protected health information for this purpose. *45 C.F.R. § 164.506(c)(1)*. If they are not part of the same covered entity, under HIPAA, the critical access hospitals may not share protected health information with DEF Medical Center or ABC Parent to facilitate the business planning of another covered entity (i.e., DEF Medical Center) absent patient authorization. *45 C.F.R. § 164.506(c)(4)*.

If the critical access hospitals, DEF Medical Center and ABC Parent were not part of the same covered entity, without regard to how the above-cited New York regulation is interpreted, New

York law would not be more stringent than HIPAA because HIPAA would require patient authorization for the data exchanges contemplated by this scenario. However, if the critical access hospitals, DEF Medical Center and ABC Parent were part of the same covered entity and no HIPAA authorization were required, the above-cited regulation would be more stringent than HIPAA if the regulation were interpreted as requiring patient consent for the exchange of information among affiliated hospitals, or between a hospital and its parent company.

Key Legal Barriers

To the extent the above-cited regulation is interpreted as requiring patient consent for the exchange of patient information among affiliated hospitals for business planning purposes, New York law would impose a barrier for affiliated hospitals that are not part of the same covered entity because it would be impractical to obtain patient consent. DOH should consider whether to provide guidance interpreting the regulation as not requiring patient consent for the exchange of data among affiliated hospitals. At a minimum, the scope of the regulation should be clarified to avoid uncertainty.

13. Bioterrorism Event

A provider sees a person who has anthrax, as determined through lab tests. The lab submits a report on this case to the local public health department and notifies their organizational patient safety officer. The public health department in the adjacent county has been contacted and has confirmed that it is also seeing anthrax cases, and therefore this could be a possible bioterrorism event. Further investigation confirms that this is a bioterrorism event, and the State declares an emergency. This then shifts responsibility to a designated state authority to oversee and coordinate a response, and involves alerting law enforcement, hospitals, hazmat teams, and other partners, as well informing the regional media to alert the public to symptoms and seek treatment if feel affected. The State also notifies the Federal Government of the event, and some federal agencies may have direct involvement in the event. All parties may need to be notified of specific identifiable demographic and medical details of each case as they arise to identify the source of the anthrax, locate and prosecute the parties responsible for distributing the anthrax, and protect the public from further infection.

Note: We assume for purposes of this analysis that the local health department will communicate the test results to the New York State Department of Health ("DOH") which will coordinate with other state agencies including the New York State Office of Homeland Security ("OHS"). Pursuant to statutory reporting requirements for laboratories, physicians and medical facilities with respect to incidents of communicable diseases, the DOH maintains an internet based communications infrastructure known as the Health Provider Network (HPN) to provide exchange of reporting, surveillance, statistical and general information between public and private health care providers. The HPN is a password protected web site.

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

If state and local government entities use electronic records, they must employ procedures and controls designed to ensure the authorization, integrity security and when appropriate, the confidentiality of the electronic records. *9 N.Y.C.R.R. § 540.5(d)*.

By Executive Order, government entities must also comply with security requirements established by the Office of Cyber Security & Critical Infrastructure Coordination ("CSCIC"). *9 N.Y.C.R.R. § 5.123*. Pursuant to CSCIC policies, all state entities are required to employ safeguards to ensure the security and confidentiality of their business information. Access to a state entity's computers, computer systems and networks must be provided through the use of individually-assigned user IDs or other technologies, such as biometrics or token cards. Each user ID must have an authentication token, such as a password, to authenticate the person accessing the data, system or network. *Cyber Security Policy P03-002.*

Discussion

DOH would appear to satisfy New York law if it employs authentication measures to verify the authority of both its employees and those of another government agency who seek access to a person's records of personal information, prior to any disclosure of electronic records to other government agencies such as OHS.

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, though they can be readily accommodated as a practical matter.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

If government entities use electronic records, they must employ procedures and controls designed to ensure the authorization, integrity security and when appropriate, the confidentiality of the electronic records. *9 N.Y.C.R.R. § 540.5(d)*.

State government entities must comply with security requirements established by CSCIC. *9 N.Y.C.R.R. § 5.123*. All state entities are required to employ safeguards to ensure the security and confidentiality of their business information. These safeguards include the use of individually assigned unique computer identifiers and other automated controls or techniques such as password protected screen savers, automated logoff procedures, or re-authentication after a set time-out period. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access.

Discussion

DOH must employ information authorization and access controls prior to any disclosure of electronic records to other government agencies such as OHS. DOH's use of the HPN requires that it must develop authentication and access control measures for those who seek access to the information contained in the HPN. The password requirement for access to HPN is one such measure.

Key Legal Barriers

New York may create some legal barriers relevant to this domain, though they can be readily accommodated as a practical matter.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Pursuant to CSCIC policies, information to be released outside a state entity or shared between state entities requires that a state entity at a minimum: (1) evaluate and document the sensitivity of the information to be released or shared; (2) identify the responsibility of each party for protecting the information; (3) define the minimum controls required to transmit and use the information; (4) record the measures that each party has in place to protect the information; (5) define a method for compliance measurement; (6) provide a signoff procedure for each party to accept responsibilities; and (7) establish a schedule and procedure for reviewing the controls. *Cyber Security Policy P03-002.*

Furthermore, use of encryption for protection of sensitive or critical information must be considered when other controls do not provide adequate protection. A secured environment must be established to protect the cryptographic keys used to encrypt and decrypt information.

Discussion

DOH must establish protocols for exchanges of information with OHS, law enforcement agencies and the federal government agencies. Depending on the sensitivity of the information being released, such as individual patient's records, DOH might have to consider additional security measures to protect confidential information such as encryption.

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, though it can be readily accommodated as a practical matter.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Under New York personal privacy protection laws, government agencies that make statutorily permitted disclosures to officers and employees of another government entity to assist with that agency's statutorily-mandated purposes or to any governmental unit performing law enforcement functions must keep an accurate accounting of the date, nature and purpose of each disclosure of a person's record of personal information and the name and address of the person or governmental unit to whom the disclosure was made. This accounting must be included in the person's record for at least five (5) years after the disclosure. *N.Y. Public Officers Law §§ 94(3)(a), (b)*.

Discussion

DOH must maintain records of disclosure and requests for disclosure of any personal information concerning a person that it discloses to other governmental agencies, such as OHS.

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, though it can be readily accommodated as a practical matter.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Clinical laboratories are required to store all records in their original form for a period of three months and may thereafter be stored on microfilm, microfiche or other photographic or electronic media. Such records must be adequately protected against destruction either by archival storage of duplicated photographic or electronic medium or by other means providing equivalent protection. *10 N.Y.C.R.R. § 58-1.11(c)*.

Government agencies that maintain a system of records must establish appropriate administrative, technical and physical safeguards to ensure the security of records. *N.Y. Public Officers Law § 94(1)(h)*.

CSCIC policy requires all state entities to implement physical and environmental security policies. Critical or sensitive information processing and storage facilities must be contained in secure areas protected by a defined security perimeter, with appropriate security barriers and some form of access controls. In addition, state entities must perform threat and risk assessments to determine evaluate and mitigate risks to security. *Cyber Security Policy P03-002.*

Discussion

The requirement under New York law that laboratories provide for protection against destruction of patient records and information is general in nature and does not add any specific obligations regarding security or confidentiality beyond those mandated under HIPAA. *See 45 C.F.R. §§ 164.308, 164.310*.

DOH must employ safeguards to ensure the confidentiality and security of its records and must perform threat and risk assessments to determine, evaluate and mitigate risks to security.

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, though it can be readily accommodated as a practical matter.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Disclosure by Laboratories
Laboratories may submit the results of any test, examination or analysis of a specimen submitted for evidence of human disease or medical condition only to a physician, his agent or other person authorized by law to employ the results in his or her practice or in fulfillment of official duties. *10 N.Y.C.R.R. § 59-1.8*. New York law requires laboratories and physicians to immediately report to the local health officer within twenty-four (24) hours by telephone, facsimile or other communication methods, positive findings or markers of certain communicable diseases including anthrax. The report must include all pertinent information such as the patient's name, date of birth, sex, address, county of residence, type and source of specimen, date collected, test results, date of final report, physician's name, address and telephone number. *N.Y. Public Health Law § 2101; 10 N.Y.C.R.R. §§ 2.1, 2.10*.

Disclosure by DOH

A state agency may not disclose a person's record or personal information unless certain exceptions apply. Disclosure is permitted pursuant to a written request or consent of that person or if specifically authorized by statute or federal rule or regulation. *N.Y. Public Officers Law §§ 96(1)(a),(f)*. The consent must specifically describe (1) the information to be disclosed, (2) the person or entity to whom such personal information is requested to be disclosed and (3) the uses for the information by the entity receiving the information. *N.Y. Public Officers Law § 96(1)(a)*. Additional exceptions exist for intra-agency disclosures if the disclosure is necessary to perform the official duties pursuant to an executive order or statutorily mandated purpose of the agency. Inter-agency disclosures are permitted where the information sought to be disclosed is necessary for the receiving governmental unit to operate a program specifically mandated by an executive order or statute and if the use for

which the information is requested is not relevant to the purpose for which it was collected. *N.Y. Public Officers Law § 96(1)(a).* In addition, disclosures to a governmental unit which performs as one of its principal functions any activity pertaining to criminal law enforcement, provided such record is reasonably described and is requested solely for law enforcement purposes. *N.Y. Public Officers Law § 96(1)(l).* Although these provisions permit disclosures by state agencies, they do not require disclosure of patients' medical records where such disclosure is not otherwise required by law. *N.Y. Public Officers Law § 96(2)(b).*

If a state of emergency is declared in response to a bioterrorism threat, the governor may, by executive order, temporarily suspend specific provisions of any statute, local law, ordinance, or orders, rules or regulations of any agency if compliance with such provisions would prevent, hinder, or delay action necessary to cope with the disaster. *N.Y. Executive Law § 29-a*. Thus, the governor could suspend certain confidentiality requirements under New York law in order to disseminate information regarding a bioterrorism attack.

Furthermore, by executive order, all state agencies are required to cooperate fully with the Director of Disaster Preparedness and Response and provide any necessary assistance to efforts to respond and recover from acts of terrorism, disasters and other emergencies, which includes establishing information sharing between and among state governments and federal governments. *9 N.Y.C.R.R. § 5.123*

Discussion

Unless one of the exceptions to the personal privacy protections applies, DOH would not have authority to disclose information to OHS or other governmental agencies. Furthermore, the disclosure exceptions to the personal privacy protection laws do not require DOH to disclose a person's medical records unless otherwise required by law. Key to any disclosure is the requirement of a statutorily mandated purpose for the receipt of necessary information. For intra-agency disclosures, DOH possesses broad general powers under New York law to "investigate the causes of disease, epidemics, the sources of mortality, and the effect of localities, employments and other conditions, upon the public health" as well as its authority to "supervise the reporting and control of disease." These investigatory powers could support an authorization to disclose within various DOH departments, a person's personal information with respect to anthrax contamination within the context of a bioterrorism threat that threatens the public health. *N.Y. Public Health Law §§ 201(1)(c), 206(1)(d).*

Inter-agency disclosure of information also require statutory authorization. Disclosures by DOH to OHS would probably fall within statutorily mandated purposes and powers granted to OHS. Under New York law, OHS is authorized to coordinate state resources for the collection and analysis of information regarding terrorist threats and activities throughout the state and also to request from any department or agency, who are also authorized, to provide such assistance, data, services as may be required by OHS in carrying out its statutory purposes, subject to applicable laws, rules and regulations. *N.Y. Executive Law § 709(2)(q).* Thus, although such disclosures would be subject to confidentiality requirements of New York personal privacy laws, the inter-agency disclosure exceptions would apply since OHS has statutory authority to receive information from DOH in accordance with its statutory powers and the disclosed information would be necessary to perform its anti-terrorism functions. In addition, assuming that OHS is considered as performing law enforcement purposes with respect to terrorism laws, which are criminal laws, DOH could also disclose personal information to OHS to further its criminal law enforcement functions, provided the information is used solely for law enforcement purposes. Such purposes could include location and prosecution of parties responsible for distributing the anthrax.

Key Legal Barriers

In order for DOH to disclose records and personal information, there must be a statutory authorization for a governmental agency to request, disclose, or receive the protected personal information. The governor could suspend certain confidentiality requirements under

New York law in order to disseminate information regarding a bioterrorism attack during a declared state of emergency.

14. Employee Health Information Scenario

An employee (of any company) presents in the local emergency department for treatment of a chronic condition that has exacerbated, which is not work-related. The employee's condition necessitates a four-day leave from work for illness. The employer requires a "return to work" document for any illness requiring more than 2 days leave. The hospital Emergency Department has an EHR and their practice is to cut and paste patient information directly from the EHR and transmit the information via email to the Human Resources department of the patient's employer.

Domain 3

Domain Description

Patient and provider identification to match identities across multiple information systems and locate electronic personal health information across enterprises.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).*

Discussion

The general duty of hospitals to keep records confidential prohibits hospitals from releasing patient information to entities unless the patient and provider status can be verified. This is consistent with HIPAA which requires covered entities to verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information, if the identity or any such authority of such person is not known to the covered entity. *45 C.F.R. § 514(h).*

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 5

Domain Description

Information protections so that electronic personal health information cannot be improperly modified.

Applicable New York Law

Hospitals are required to employ "safeguards to ensure safety and confidentiality." 10 N.Y.C.R.R. 405.10(c).

Discussion

This requirement under New York law is general in nature and does not exceed HIPAA requirements.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Public Health Law § 18(6) requires the tracking and documentation by licensed professionals of certain disclosures to third parties (including initial disclosures to government and private payers). Either a copy of the subject's written authorization or the name of and address of such third party and a notation of the purpose of the disclosure must be indicated in the patient's file. Exceptions exist for facility staff and contractors, and government agencies for the purposes of facility inspections or professional conduct investigations.

Discussion

Public Health Law § 18(6) law requires additional tracking of disclosures by licensed professionals than is required under HIPAA. This provision requires tracking of disclosures made to external parties (including providers) not under contract with the disclosing provider, for initial payment disclosures to payers and for other disclosures not explicitly exempted in the law.

Key Legal Barriers

New York law requires additional administrative logging for disclosures by licensed providers beyond HIPAA mandates.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Hospitals must employ safeguards to ensure the security and confidentiality of their medical records. *10 N.Y.C.R.R. § 405.10(c)(4)*.

Hospitals must adopt policies and procedures to ensure the security of electronic or computer equipment from unwarranted access. *10 N.Y.C.R.R. § 405.10(c)(4)(iii)*.

Health care providers and health care facilities must adopt protocols for ensuring that records (including electronic records) containing HIV-related information are maintained securely and used for appropriate purposes. *10 N.Y.C.R.R. § 63.9(d)*.

Discussion

The requirement under New York law that hospitals employ safeguards to ensure the confidentiality and security of their medical records is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. The same is true of the requirement under New York law that protocols be adopted to ensure records containing HIV-related information are securely maintained and appropriately used. The requirement under New York law that hospitals adopt policies and procedures to prevent unwarranted access to computer equipment is consistent with HIPAA. See *45 C.F.R. §§ 164.308, 164.310*.

The implementation of HIPAA-compliant safeguards, policies and procedures would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Hospitals are required to ensure the confidentiality of medical records. Information contained in such records may be released only to hospital staff involved in treating the patient "and individuals as permitted by Federal and State laws." *10 N.Y.C.R.R. § 405.10(a)(6).* This regulation requires hospitals to obtain consent from the patient prior to disclosing medical records to an outside entity, even for treatment or reimbursement purposes. See also, *Williams v. Roosevelt Hospital, 66 N.Y.2d 391(1985)*. Physicians also are prohibited from disclosing identifiable information without consent, except if authorized or required by law. *Education Law §6530(23) and 8 N.Y.C.R.R. § 29.* Such state required consent may be a general consent permitting certain types of disclosures, and the consent does not have to be as specific as a HIPAA authorization or contain all of the HIPAA-mandated elements. If consent is oral or implied, it should be documented in the chart to enable enforcement and minimize litigation risk.

New York law permits medical services to be rendered without consent when in the physician's judgment an emergency exists and the person is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk

to the person's life or health. *N.Y.P.H.L § 2504(4).* This provision has been interpreted to allow release of medical information under such circumstances, as well.

Health care providers may not disclose HIV-related information without the patient's authorization except for certain specifically defined purposes. *N.Y. Public Health Law Article 27-F*. In cases where the patient's authorization is required, the provider may not rely on a general consent; it must obtain a special HIV release that expressly references the nature of the information being disclosed and contains certain mandated elements. *N.Y. Public Health Law § 2780(9)*. The specific release form must be developed by DOH or approved by DOH. *10 N.Y.C.R.R. § 63.5(a)*.

Discussion

New York law is consistent with HIPAA because it requires patient consent for the disclosure of protected health information by hospitals to an employer. Such disclosures require patient authorization under HIPAA. See *45 C.F.R. § 164.508*.

At a minimum, New York law would require the hospital to obtain a general consent from each patient prior to submitting an email containing information from the EHR to the employer and perhaps to narrowly tailor the email to include relevant information regarding the ability to return to work and not the entire record in the hospital's EHR. Most New York hospitals obtain a general consent from each patient as part of the admission or registration process. However, the language in the consent form may be narrowly tailored to permit the hospital to submit a "return to work" document. A hospital would have to carefully review its consent form to determine whether the language is sufficiently broad to permit disclosure of the patient's personally identifiable information in the EHR.

In addition, to the extent an EHR contains HIV-related information, the hospital would have to obtain a more specific authorization from any patient whose EHR contained HIV-related information prior to the transmission.

Key Legal Barriers

Absent the presence of HIV information, New York law does not create any additional legal barriers relevant to this domain because patient authorization for the transmissions is required under HIPAA.

15. Public Health-Scenario A

A patient with active TB, still under treatment, has decided to move to a desert community that focuses on spiritual healing, without informing his physician. The TB is classified MDR (multi-drug resistant). The patient purchases a bus ticket - the bus ride will take a total of nine hours with two rest stops across several states. State A is made aware of the patient's intent two hours after the bus with the patient leaves. State A now needs to contact the bus company and other states with the relevant information.

Note: We assume that State A is New York. We also assume that the contacts will be made by a government agency of New York such as the New York State Department of Health ("DOH").

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

If state and local government entities use electronic records, they must employ procedures and controls designed to ensure the authorization, integrity security and when appropriate, the confidentiality of the electronic records. *9 N.Y.C.R.R. § 540.5(d)*.

By Executive Order, government entities must also comply with security requirements established by the Office of Cyber Security & Critical Infrastructure Coordination ("CSCIC"). *9 N.Y.C.R.R. § 5.123*. Pursuant to CSCIC policies, all state entities are required to employ safeguards to ensure the security and confidentiality of their business information. Access to a state entity's computers, computer systems and networks must be provided through the use of individually-assigned user IDs or other technologies, such as biometrics or token cards. Each user ID must have an authentication token, such as a password, to authenticate the person accessing the data, system or network. *Cyber Security Policy P03-002.*

Discussion

DOH would appear to satisfy New York law if it employs authentication measures to verify the authority of both its employees and those of another government agency who seek access to a person's records of personal information, prior to any disclosure of electronic records to other government agencies.

Key Legal Barriers

New York law requires authentication and security measures that could create legal barriers relevant to this domain, but can be readily accommodated as a practical matter.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

If government entities use electronic records, they must employ procedures and controls designed to ensure the authorization, integrity security and when appropriate, the confidentiality of the electronic records. *9 N.Y.C.R.R. § 540.5(d)*.

State government entities must comply with security requirements established by CSCIC. *9 N.Y.C.R.R. § 5.123*. All state entities are required to employ safeguards to ensure the security and confidentiality of their business information. These safeguards include the use of individually assigned unique computer identifiers and other automated controls or techniques such as password protected screen savers, automated logoff procedures, or re-authentication after a set time-out period. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access.

Discussion

In order to comply with New York law, DOH must employ information authorization and access controls for any electronic records it maintains.

Key Legal Barriers

New York law may creates some legal barriers relevant to this domain, but can be readily accommodated as a practical matter.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Pursuant to CSCIC policies, information to be released outside a state entity or shared between state entities requires that a state entity at a minimum: (1) evaluate and document the sensitivity of the information to be released or shared; (2) identify the responsibility of each party for protecting the information; (3) define the minimum controls required to transmit and use the information; (4) record the measures that each party has in place to protect the information; (5) define a method for compliance measurement; (6) provide a signoff procedure for each party to accept responsibilities; and (7) establish a schedule and procedure for reviewing the controls. *Cyber Security Policy P03-002*.

Furthermore, use of encryption for protection of sensitive or critical information must be considered when other controls do not provide adequate protection. A secured environment must be established to protect the cryptographic keys used to encrypt and decrypt information.

Discussion

DOH must establish protocols for exchanges of information. Depending on the sensitivity of the information being released, such as individual patient's records, DOH might have to consider additional security measures to protect confidential information such as encryption.

Key Legal Barriers

New York law may creates some legal barriers relevant to this domain, but can be readily accommodated as a practical matter.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Under New York personal privacy protection laws, government agencies that make statutorily permitted disclosures to officers and employees of another government entity to assist with that agency's statutorily-mandated purposes or to any governmental unit performing law enforcement functions must keep accurate accountings of the date, nature and purpose of each disclosure of a person's record of the personal information and the name and address of the person or governmental unit to whom the disclosure was made. This accounting must be included in the person's record for at least five (5) years after the disclosure. *N.Y. Public Officers Law § 94(3)(a), (b)*.

Discussion

The definition for "governmental agencies" under New York's privacy protection laws includes another state's governmental entities. Thus, DOH must maintain records of any authorized disclosures of personal information concerning a person's TB status that it discloses to another state's governmental agencies

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, but can be readily accommodated as a practical matter.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Government agencies that maintain a system of records must establish appropriate administrative, technical and physical safeguards to ensure the security of records. *N.Y. Public Officers Law § 94(1)(h)*.

CSCIC policy requires all state entities to implement physical and environmental security policies. Critical or sensitive information processing and storage facilities must be contained in secure areas protected by a defined security perimeter, with appropriate security barriers and some form of access controls. In addition, state entities must perform threat and risk assessments to determine evaluate and mitigate risks to security. *Cyber Security Policy P03-002.*

Discussion

DOH must employ safeguards to ensure the confidentiality and security of its records and must perform threat and risk assessments to determine evaluate and mitigate risks to security.

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, but may be readily accommodated as a practical matter.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

Reports of patients afflicted with TB and all such patients' records of examination are confidential and not open to inspection by any other person other than the state or local health authorities. These health officers may not permit the disclosure of the identity of such person except as may be authorized in the New York Sanitation Code. *N.Y. Public Health Law § 2221*. A state or local health officer authorized to receive laboratory or other reports relating to cases of TB may disclose information contained in such reports only when in his or her judgment it will serve the best interest of the patient or his or her family, or contribute to the protection of the public health. Furthermore, the officer may, subject to the foregoing purposes, permit access to such reports by representatives of official or non-official agencies concerned with the control of tuberculosis. *10 N.Y.C.R.R. § 2.17*. Enforcement provisions under New York law require a health officer to investigate any allegations that a person afflicted with TB is acting in a dangerous or careless manner that exposes others to danger of infection. *N.Y. Public Health Law § 2120*. The statute does not specifically mention what disclosures would be permitted in the course of this investigation.

Disclosure of personal information by a state agency is subject to confidentiality requirements, subject to certain exceptions. A state agency may not disclose any record or personal information regarding a person unless such disclosure is pursuant to a written request or consent of that person or if specifically authorized by statute or federal rule or regulation. *N.Y. Public Officers Law §§ 96(1)(a),(f)*. The consent must specifically describe (1) the information to be disclosed, (2) the person or entity to whom such personal information is requested to be disclosed and (3) the uses for the information by the entity receiving the information. *N.Y. Public Officers Law § 96(1)(a)*. Disclosures between government entities, including those of another state, are permitted where the information sought to be disclosed is necessary for the receiving governmental unit to operate a program specifically mandated by an executive order or statute and if the use for which the information is requested is not relevant to the purpose for which it was collected. *N.Y. Public Officers Law § 96(1)(a).* In addition, disclosures to a governmental unit that performs criminal law enforcement activities as one of its principal functions is permitted, provided such record is reasonably described and is requested solely for law enforcement purposes. *N.Y. Public Officers Law § 96(1)(l).* Although these provisions permit disclosures by state agencies, they do not require disclosure of patients' medical records where such disclosure is not otherwise required by law. *N.Y. Public Officers Law § 96(2)(b).*

Discussion

Unless one of the personal privacy protection law exceptions applies, DOH would not have authority to disclose information to another state's governmental agencies. Key to any disclosure by a state agency is the requirement of a statutorily-mandated purpose for the receipt of necessary information. One exception, which authorizes disclosure if required by law, necessitates examining DOH's powers under New York law regarding communicable diseases. DOH's broad powers to "investigate the causes of disease, epidemics, the sources of mortality, and the effect of localities, employments and other conditions, upon the public

health" as well as its authority to "supervise the reporting and control of disease" could authorize disclosure of a patient's personal information and medical records. *N.Y. Public Health Law §§ 201(1)(c), 206(1)(d)*. A person afflicted with active MDR TB who travels interstate without informing his physician poses a danger of infection that would give rise to the local health officer and the health officer's duty to investigate. Arguably, despite the confidentiality of tuberculosis patient records and reports, the public health officer could disclose the patient's identity and TB status to another state's government health entities, and if necessary to investigate the case, to non-official entities, such as the bus company, despite the confidential nature of records for patients with tuberculosis, if a health officer believed it necessary to protect the public health. However, in most cases, non-official entites will not need to know the specific diagnosis of the person, but only that they have a communicable disease which requires locating information.

Additionally, disclosures between government agencies of multiple states is permitted where the receiving entity requests information that is necessary and pursuant to statutorily-mandated purposes or for law enforcement purposes. Any disclosures by DOH to another state's government agency would need to satisfy this requirement.

Key Legal Barriers

In order for DOH to disclose and for another state's governmental agencies to request and receive necessary personal information regarding a patient, there must be a statutory authorization. Health officers have discretion to disclose information necessary to protect the public's health, which might permit disclosure of certain information to the bus company. However, because the bus company is not an entity specified in the exceptions to the New York personal privacy protection laws, there would probably be some limitations on what information could be disclosed.

16. Public Health-Scenario B

A newborn's screening test comes up positive for a state-mandated screening test and the state lab test results are made available to the child's physicians and specialty care centers specializing in the disorder via an Interactive Voice Response system. The state lab also enters the information in its registry, and tracks the child over time through the child's physicians. The state public health department provides services for this disorder and notifies the physician that the child is eligible for those programs.

Note: In New York, the state lab is the Wadsworth Center Laboratory, operated by the New York State Department of Health. *10 N.Y.C.R.R. § 69-1.1(a).*

Domain 1

Domain Description

User and entity authentication is used to verify that a person or entity seeking access to electronic protected health information is who they claim to be.

Applicable New York Law

There are no relevant laws regarding disclosure by private physicians.

If state and local government entities use electronic records, they must employ procedures and controls designed to ensure the authorization, integrity security and when appropriate, the confidentiality of the electronic records. *9 N.Y.C.R.R. § 540.5(d)*.

By Executive Order, government entities must also comply with security requirements established by the Office of Cyber Security & Critical Infrastructure Coordination ("CSCIC"). *9 N.Y.C.R.R. § 5.123*. Pursuant to CSCIC policies, all state entities are required to employ safeguards to ensure the security and confidentiality of their business information. Access to a state entity's computers, computer systems and networks must be provided through the use of individually-assigned user IDs or other technologies, such as biometrics or token cards. Each user ID must have an authentication token, such as a password, to authenticate the person accessing the data, system or network. *Cyber Security Policy P03-002.*

Discussion

The New York State Department of Health ("DOH") would appear to satisfy New York law if it employs authentication measures to verify the authority of its employees prior to any disclosure of electronic records for intra-agency transmissions between the state lab and DOH.

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, though they can be readily accommodated as a practical matter.

Domain 2

Domain Description

Information authorization and access controls to allow access only to people or software programs that have been granted access rights to electronic personal health information.

Applicable New York Law

If government entities use electronic records, they must employ procedures and controls designed to ensure the authorization, integrity security and when appropriate, the confidentiality of the electronic records. *9 N.Y.C.R.R. § 540.5(d)*.

State government entities must comply with security requirements established by CSCIC. *9 N.Y.C.R.R. § 5.123*. All state entities are required to employ safeguards to ensure the security and confidentiality of their business information. These safeguards include the use of individually assigned unique computer identifiers and other automated controls or techniques such as password protected screen savers, automated logoff procedures, or re-authentication after a set time-out period. The safeguards must include policies and procedures that restrict access to information to those individuals who have the need, a reason and permission for such access.

Discussion

DOH must employ information authorization and access controls prior to any disclosure of electronic records to an intra-government agency such as the state lab.

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, though they can b readily accommodated as a practical matter.

Domain 4

Domain Description

Information transmission security or exchange protocols (i.e., encryption, etc.) for information that is being exchanged over an electronic communications network.

Applicable New York Law

Pursuant to CSCIC policies, information to be released outside a state entity or shared between state entities requires that a state entity at a minimum: (1) evaluate and document the sensitivity of the information to be released or shared; (2) identify the responsibility of each party for protecting the information; (3) define the minimum controls required to transmit and use the information; (4) record the measures that each party has in place to protect the information; (5) define a method for compliance measurement; (6) provide a signoff procedure for each party to accept responsibilities; and (7) establish a schedule and procedure for reviewing the controls. *Cyber Security Policy P03-002.*

Furthermore, use of encryption for protection of sensitive or critical information must be considered when other controls do not provide adequate protection. A secured environment must be established to protect the cryptographic keys used to encrypt and decrypt information.

Discussion

DOH must establish protocols for exchanges of information. Depending on the sensitivity of the information being released, such as individual patient's records, DOH might have to consider additional security measures to protect confidential information such as encryption.

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, though they can be readily accommodated as a practical matter.

Domain 6

Domain Description

Information audits that record and monitor the activity of health information systems.

Applicable New York Law

Under New York personal privacy protection laws, government agencies that make statutorily permitted disclosures to officers and employees of another government entity must keep accurate accountings of the date, nature and purpose of each disclosure of a record or the personal information and the name and address of the person or governmental unit to whom the disclosure was made. This accounting must be included in the person's record for at least five (5) years after the disclosure. *N.Y. Public Officers Law §§ 94(3)(a), (b)*.

Discussion

DOH must maintain records of any disclosures of information concerning a newborn's medical records that it discloses to other governmental agencies. New York law does not impose any specific obligations regarding the timing or nature of the mandated audits.

Key Legal Barriers

New York law may create some legal barriers relevant to this domain, though they can be readily accommodated as a practical matter.

Domain 7

Domain Description

Administrative or physical security safeguards required to implement a comprehensive security platform for health IT.

Applicable New York Law

Government agencies that maintain a system of records must establish appropriate administrative, technical and physical safeguards to ensure the security of records. *N.Y. Public Officers Law § 94(1)(h)*.

CSCIC policy requires all state entities to implement physical and environmental security policies. Critical or sensitive information processing and storage facilities must be contained in secure areas protected by a defined security perimeter, with appropriate security barriers and some form of access controls. In addition, state entities must perform threat and risk assessments to determine evaluate and mitigate risks to security. *Cyber Security Policy P03-002.*

Discussion

The requirement under New York that health care providers employ safeguards to ensure the confidentiality and security of their medical records is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. The requirement under New York law that protocols be adopted to ensure records containing HIV-related information are securely maintained and appropriately used is general in nature and does not add any specific obligations beyond what is required under the HIPAA privacy and security regulations. See *45 C.F.R. §§ 164.308, 164.310*.

The requirement that DOH employ safeguards to ensure the confidentiality and security of its records is also general in nature and does not delineate specific measures that DOH must take regarding security and confidentiality.

The implementation of HIPAA-compliant safeguards, policies and procedures would appear to satisfy New York law.

Key Legal Barriers

New York law does not create any legal barriers relevant to this domain beyond requirements under HIPAA.

Domain 8

Domain Description

State law restrictions about information types and classes, and the solutions by which electronic personal health information can be viewed and exchanged.

Applicable New York Law

The newborn screening statute and regulations require collaboration and data-sharing between the facility where a child is born, the state lab, the infant's primary health care provider and the specialized care centers. *N.Y. Public Health Law § 2500-a; 10 N.Y.C.R.R. Subpart 69-1.* Pursuant to the newborn screening regulations, the responsible physician for the newborn must arrange for diagnostic evaluation and case management with an approved specialized care center for confirmed abnormal test results. In addition, for newborns who test positive for HIV antibodies, the responsible physician must also arrange for health care, case management and other social services as needed for the newborn. *10 N.Y.C.R.R. § 69-1.5(g).* There is no mandated newborn screening for any infant whose guardian notifies the facility where the child is born of membership in a recognized religious organization whose teachings and tenets are contrary to newborn screening. *N.Y. Public Health Law § 2500-a(b).*

Physicians are prohibited from revealing personally identifiable facts, data, or information obtained in a professional capacity without the prior consent of the patient, except as authorized or required by law. *N. Y. Education § 6530(23).* Newborn screening regulations require that in addition to the submission of specimens for screening of certain diseases, the chief executive officer of a hospital or the responsible physician caring for the newborn must also submit identifying information concerning the newborn, the mother, the hospital and the physician to the DOH in an "approved and validated electronic format." *10 N.Y.C.R.R. § 69-1.3.* The newborn screening test results are to be included in the infant's permanent health record.

In addition, newborn HIV testing regulations mandate the security and confidentiality of these results in the medical record of the newborn in accordance with New York law. Pursuant to HIV confidentiality and disclosure laws, health care providers may not disclose HIV-related information without the patient's authorization except for certain specifically defined purposes. *N.Y. Public Health Law Article 27-F*. In cases where the patient's authorization is required, the provider may not rely on a general consent. Rather, the provider must obtain a special HIV release that expressly references the nature of the information being disclosed and contains certain mandated elements. *N.Y. Public Health Law § 2780(9)*. The specific release form must be developed by DOH or approved by DOH. *10 N.Y.C.R.R. § 63.5(a)*. The permitted purposes include disclosure to a health care provider or health facility when knowledge of the of HIV related information is necessary to provide appropriate care or treatment to the protected individual, a child of the individual or person authorized to consent to health care for the person. *N.Y. Public Health Law § 2782(1)(d).*

In addition, for newborn HIV screening tests, the chief executive officer of the hospital must transmit to the responsible physician a copy of the newborn's HIV test result and, at the request of the responsible physician, also transmit the result to an HIV specialized care center. *10 N.Y.C.R.R. § 69-1.3(l).* Furthermore, the chief executive officer of a hospital must ensure that the data for patient follow-up for HIV positive newborns must be collected and provided to authorized staff at the DOH as well as submit information to the DOH on the prior HIV testing and treatment history of the mother for the purposes of medical audits, provided such information is kept confidential. *10 N.Y.C.R.R. § 69-1.3(l)*.

Hospitals and birth centers must ensure the transfer to the newborn's medical record of a mother's HIV test result. *N.Y.C.R.R. §§ 405.21, 754.7, 754.8.*

Discussion

The newborn screening regulations require collaboration and sharing of information between the testing laboratory at DOH, the physician and the specialized care centers for newborns who test positively for certain diseases. Physicians are required by statute to arrange and consult with specialists and other social service agencies for diagnostic evaluation and case management with approved specialized centers for the follow-up process associated with particular diseases. The amount of initial consultation and initial disclosure depends on the severity of the condition and the extent to which specialized care is needed. For this initial diagnosis and follow-up for treatment, no consent from the newborn's parents or guardians is required because this is part of a mandated newborn screening process, unless the family provides notice of membership in a recognized religious organization opposed to newborn screening.

DOH's Newborn Screening Program currently only requires the newborn's physician to report the newborn's initial diagnosis as a follow-up to a positive newborn screening test result. Additional information exchanges for "tracking" and "follow-up reviews" could be mandated by regulation in the future. *N.Y. Public Health Law § 2500-a(a).*

Key Legal Barriers

To the extent future disclosures by a physician are not considered part of the initial diagnosis and follow-up after a newborn screening, additional regulation or consent from the newborn's parents would probably be required.