

HISPC Legal Work Group Scenario Analysis

It is suggested that you read a scenario from the [wiki](#) and then the corresponding scenario analysis that follows in this document.

Then you may make comments on the wiki, using the link <https://hispc.pbwiki.com/Scenarios?login=1> to log in. Please cite the scenario and the column & items from the analysis you are referencing. *You may find it helpful to print out the scenarios for reference.*

The analysis of the 18 Scenarios is presented in the following pages as worksheets. Some pages, due to the length and depth of the analysis spill over 1 page, as indicated below.

Scenario found on	Page
1	2
2	3
3	4
4	5
5	6-7
6	8
7	9-10
8	11
9	12
10	13
11	14
12	15-16
13	17
14	18-19
15	20
16	21-22
17	23
18	24

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
1	Patient Care Scenario A	1) Requirement for individual/user authentication in the request for patient information for previous treatment.	There is no legal obstacle to obtaining information from a prior hospitalization when it is needed by the emergency room physician for diagnosis and treatment. According to the scenario, the hospital is in a neighboring state so there would be sharing across the state line. HIPAA clearly allows this as part of the treatment exception and there is nothing in Ohio law that would prevent this request for information. The neighboring state may want a signed consent form to send the information. (We don't know what the neighboring state would require before releasing information) . Additionally, ORC 5122.31 addresses the release of information regarding mental health hospitalizations.	1 - 9	Hospitals, Physicians, Clinicians, Pharmacy, Behavior Health	1) Lack of a required standard identifier such as a patient identifier number	45 CFR 164.312 (d) ORC 5122.31	The neighboring state may have restrictions on the release of mental health information similar to Ohio's that might be a barrier.
						2) Lack of standardized transmission and integrity controls	45 CFR 164.312 (e) HIPAA 45 CFR 164.510 may be a temporary solution/exception that would allow the daughter to assist with decisions about the mother's health care	None
						3) Lack of certification - NIST Standard	45 CFR 164	None
		2) Accounting of protected health information disclosures	The reluctance to release (or re-release) PHI created by another entity is a pervasive problem based on a firm belief that it is prohibited. However, we are not aware of any legal basis for this position unless the information to be released pertains to mental health issues, drug and alcohol issues or research protocols. Thus it is a barrier, but not a legal barrier.			4) Legal status of the patients daughter?	If the patient is confused to the point that she cannot give consent, her adult daughter does not have status in Ohio to provide consent unless the adult daughter has a guardianship or has a durable power of attorney for health care. That is the neighboring state's issue and may present a practical problem with getting the information to the ER doctor. Additionally, HIPAA 45 CFR 164.510 may be a temporary solution/exception that would allow the daughter to assist with decisions about the mother's health care.	None
						5) Varying standards for phone/fax requests	None	None
						6) National "system of truth" needed to manage authorization	None	None
						7) Can patient opt-out of national data repository or limit access to data?	RC 3701.24	None

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
2	Patient Care Scenario B	Requirement for entity authentication to validate request for information.	Virtually all substance abuse treatment facilities are covered under the Federal Drug and Alcohol Confidentiality Act (42 CFR Part 2), which is stricter than HIPAA in this instance. IF THE CLIENT'S AUTHORIZATION CANNOT BE OBTAINED, A Qualified Service Organization/Business Associate Agreement must be entered into between treatment facility and primary care provider prior to disclosure (42 CFR § 2.12 (c)(4), 45 CFR § 160.103, § 164.504(e)). Primary care provider cannot disclose records from substance abuse treatment facility to the specialist without the patient's authorization due to 42 CFR Part 2 and Ohio law prohibition on redisclosure (42 CFR § 2.32, OAC 3793:2-1-06(H)).	1 - 9	Hospitals, Clinicians, Pharmacists Physicians, Behavioral Health Providers, Payers	1) Lack of standardized transmission and integrity controls	45 CFR 164.312 (d)	Possible diminished capacity to execute consent upon admission to substance abuse program
						2) Lack of certification - NIST Standard	45 CFR 164.312 (e)	
						3) Not permitted to send substance treatment data with other records	ORC 3793.13	
						4) Can email be used to send data in lieu of a fax?	None	
						5) Revised code speaks to primary care physicians responsibility	See Legal Review	
							Miscellaneous: Required elements in authorization form - 42 CFR § 2.31(a), 45 CFR §164.508(c), ORC 3793.13, OAC 3793:2-1-06(G)	

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
3	Patient Care Security and Access Scenario C	1) Assignment of user identification and password.	See response to obstacle no. 1	1 - 9	Hospitals, Long-Term Care, Clinicians, Physician Groups, Payers, Behavioral Health, Pharmacies	1) Lack of a required standard identifier such as a patient identifier number	45 CFR 164.312 (d). An obstacle exists but can be mitigated by implementation of the National Provider Identifier mandated under 45 CFR 162, Subpart D. Furthermore, development and implementation of unique health identifiers for individuals, employers and health plans mandated under Section 1173 of Subtitle F of HIPAA, will help to mitigate the obstacle.	
		2) Access authorization to behavior health unit.	45 CFR 164.310. Not an obstacle. The BHU would need to ensure its physical access controls satisfy the HIPAA physical safeguards requirements, which could also help the unit satisfy Ohio law; ORC Section 3701.75, ORC Section 5122.31 and OAC Section 3701-17-19.			2) Lack of standardized transmission and integrity controls	Yes this is an obstacle but not a legal obstacle as there is an absence of a mandated standards. HIPAA required standards are limited to electronic exchange of claims and payment info, and do not address standards for other components of the medical record; some provisions of Ohio law address requirements for security and integrity controls, but do not set standards, see e.g. ORC 3701.75 (appl. to electronic medical records), OAC 5122-27-09 (appl. to providers of ODMH certified MH services)	
		3) Standardized authentication and registration process.	See response to obstacle no. 5			3) Do internal policies for encryption apply to off shore entity?	HIPAA requires CE to have business associate agreement (BAA) with an entity to whom it supplies access to PHI for purposes of performing function on behalf of the CE; security requirements, including encryption obligations, should be passed on via BAA (though there is no standard re: encryption mechanism); ORC 2307.39 provides for enforcement of choice of Ohio law contractual provision	
						4) Inconsistent use of electronic health record	An obstacle exists because of the lack of requirements to utilize electronic health records compounded by the lack of interoperability standards or requirements with respect to the use of electronic health records. Major obstacle to forced implementation is the cost. Implementation of 42 CFR 1001.952(x) and (y) and 42 CFR 411.357(v) and (w) will assist with implementation but broader adoption of interoperable EHRs may be difficult.	
						5) Practicality of a single standard for accessing records	Yes, this is an obstacle. Currently no standard access requirements. HIPAA security mandates are technology neutral. Interoperability discussion is also focused on technology neutral solutions. Existence of hundreds if not thousands of information systems in the industry with customization pursuant to entity needs will make standardization difficult.	
						6) Lack of a translator to handle all standards	45 CFR 160.103. Yes, this is an obstacle because there are no national standards for non-claims related PHI, but HIPAA does allow health care clearinghouses that could act as a single translator to handle standard records disclosures.	
						7) Develop a federated repository with RHIO responsible for implementation	45 CFR Parts 160, 162, 164. Not an obstacle, but must comply with applicable federal and complicated mix of state medical records content and use regulations applicable to various providers (e.g., Hospitals, Nursing Facilities, Behavioral Health).	
						8) National standards for access to Psych records	Yes this is a legal obstacle as Ohio law has strict standards that will be applicable. HIPAA sets forth access requirements that apply on a national level, but these are only applicable to covered entities (and their business associates), and the regulations do not preempt more stringent provisions of state law; Ohio mental health law contains several provisions that are more stringent than HIPAA regs - see ORC 5122.31	
						9) Access to electronic health records diminishes with national repository	Yes, is an obstacle without a new national standard for psych records disclosure. Also, a national repository could be an obstacle for patient access. For example, HIPAA patient access standards are different than patient access standards for hospital and health care practitioner records under state laws. See O.R.C.. 3701.74	

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
4	Patient Care Scenario D	1) Requirement for individual/user authentication in the request for patient information for previous treatment.	There is no legal obstacle to obtaining information from another health care entity. HIPAA allows for such a transfer of PHI. 45 CFR 164.506. According to the scenario, the hospital is in a neighboring state so there would be sharing across the state line. HIPAA clearly allows this as part of the treatment exception and there is nothing in Ohio law that would prevent this request for information. The neighboring state may want a signed consent form to send the information. (we don't know what the neighboring state would require before releasing information)	1 - 9	Hospitals, Clinicians, OtherCare Providers, Government, Behavior Health, Public Health	1) Lack of a required standard identifier such as a patient identifier number	RC 370124 written consent	
		2) Dissemination of data involving behavioral health issues.	Regarding genetic information, currently there is no law that addresses this aspect of the scenario. The release of HIV information would be governed by RC 3701.243. Information regarding a deceased individual, may only be released with the approval of the deceased person's estate.			2) Lack of standardized transmission and integrity controls	45 CFR 164.506	None
						3) Alerts to physician and providers of special precautions	45 CFR 164.312 (d)	None
						4) Pharmacy standards for HIV patients	45 CFR 164.312 (e)	None
						5) Verifying that the correct patient is being treated	None	None
						6) Release information but restrict viewer from seeing HIV status because data is public information	RC 3701.243	None
						Regarding releasing information created by another care provider, this may be a barrier, but not a legal barrier. HIPAA calls anything that the covered entity creates or maintains as health information. We are not aware of a legal cite for saying that an institution should only produce the information that it creates, so we are not sure about liability issues. We do know that most physician offices and hospitals have an internal policy that states they will only give information that they create. If they obtain test results from another site (physician office or IDTF) they tell the patient to get the information from the original site. We are not aware that this is a legal requirement. We have only seen it as an institutional policy.		

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
5	Payment Scenario	1) Requirement for person or entity authentication	Obstacle # 1 and Procedure #2: Provided covered entities comply with existing statutes and regulations, this obstacle is not a legal barrier. X Health Payer (other than worker's compensation) and Health care provider are both covered entities. 45 CFR 160.103. Request for, use and disclosure of E.H.R is subject to minimum necessary standard, 45 CFR 164.502(b), unless authorization is obtained. 45 CFR 502(b)(2)(iii). X Health Payer must establish policies or procedures to ensure request and use complies with minimum necessary standard. 45 CFR 164.514(d)(2), (4). Health care provider must establish policies or procedures to ensure disclosure complies with minimum necessary standard. 45 CFR 164.514(d)(3). Health care provider may reasonably rely on request of X Health Payer as the minimum necessary. 45 CFR 164.514(d)(3)(iii)(B). Entire medical record may not be requested or disclosed unless specifically justified as reasonably necessary. 45 CFR 164.514(d)(5).	1 - 9 excluding 8	Payers, Consumers, State Government, Clinicians, Hospitals	1) Data access must be limited to minimum necessary	See discussion under Legal Review and Other Legal Barriers.	Authorization is required under HIPAA for psychotherapy notes. 45 CFR 514(d)(2). Ohio law prohibits disclosure of HIV status without authorization. O.R.C. 3701.243. State workers compensation statute governs disclosure for WC benefits. 45CFR 512(l); O.A.C §4123-6-20(D).
		2) Data access must be limited to minimum necessary	Obstacle # 2: Provided covered entities comply with existing regulations, this obstacle is not a legal barrier. Covered entities are required to implement security standards, including technical safeguards to ensure the confidentiality and integrity of PHI transmitted electronically. 45 CFR 164.312(e) (1).			2) Lack of standardized transmission and integrity controls	See discussion under Legal Review.	Minimum necessary standard would also apply.
			Obstacle #3: Not a legal barrier. A provider and health plan would need to address the terms of the health plan's data access and limits thereof in its participating provider agreement with the health plan. The transmission of data electronically would need to meet 45 CFR Part 162 requirements for transmitting electronic referral information (162.1301) and other standards as required, including the minimum necessary standard.			3) Limitation on data access by contract	See discussion under Legal Review and Other Legal Barriers.	Must also comply with O.R.C. 1751.13, which requires that the contract between the health plan and the provider address access and confidentiality of medical records and health information.
			Obstacle #4 and Procedure #1: Possibly a legal barrier as this policy/procedure may not satisfy the requirement for security safeguards to protect the privacy of the patient information. The risk of unauthorized access based on undocumented verbal authorization seems unlikely to meet the standard in 45 CFR 164.308.			4) Plans have access through verbal authorization	See discussion under Legal Review.	
			Obstacle #5: Not a legal barrier so long as sufficient security safeguards, policies and procedures can be put in place to protect the privacy of the patient information. The role of each person or position accessing the information would need to be evaluated and that person's access would need to be limited to that information which is appropriate for the specific role or function. See 45 CFR 164.300 et. al. and 45 CFR 164.308, 45 CFR 164.514(d)(4)			5) Limiting access through varying roles	See discussion under Legal Review.	
			Obstacle #6: Not certain how this is an obstacle under HIPAA (?) Both "Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services" and "Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges" are defined as "Payment" activities for which an authorization is not required. Case management and UR staff could both fall under "payment; access under this scenario is being requested for case management staff. Customer and/or provider rights to further review of health plan decision [utilization review activities; see e.g. O.R.C. 1751.77 to 1751.88] may be hampered by lack of access to the records the health plan reviewed in making its initial determination unless additional access is also granted to the provider's electronic record.			6) Separation of active case management from review process	See discussion under Legal Review and Other Legal Barriers.	"Minimum necessary" is an issue for each activity. In workers' compensation, parties have rights of appeal on treatment issues from Managed Care Organization (MCO) to the Bureau of Workers' Compensation and to the Industrial Commission [See OAC 4123-6-16; O.R.C. 4123.511] Lack of access to records the MCO reviewed in making its initial determination may pose due process problems, since Ohio WC is a governmental function.

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
			Obstacle #7: Health plan may provide for access to records by contract with provider [See, e.g., O.R.C. 1751.13(C)(5)]. Providers have statutory duty to cooperate with health plan utilization review procedures. O.R.C. 1751.822. Contract could conceivably specify penalty/termination for failure to comply with medical record access terms and statutory duties.			7) Rules for handling providers who refuse to give data upon request	See discussion under Legal Review and Other Legal Barriers.	Workers' compensation rule requires providers to submit documentation [OAC 4123-6-20(D)]; currently does not specify format. Providers may be decertified from workers' comp participation for failure to comply with WC rules [See OAC 4123-6-02.5(B); OAC 4123-6-17]

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
6	RHIO Scenario	Release of information for research purposes	Release of information is not for research purposes but for information sharing. It is not clear from the scenario that any research will be performed.	1 - 9 excluding 8	Hospitals, Clinicians, Pharmacy, Medical and Public Health Schools	1) Research must fall under authority of an IRB	45 CFR 164.512 (l); See comments under Legal Review. HIPAA research use and disclosure rules are not applicable if this is not research. There do not appear to be any barriers to the exchange of information in this scenario provided that the RHIO participants follow all applicable law (HIPAA privacy and security requirements) that may come into play depending on how the RHIO is structured and the functions it performs. Privacy and security concerns not specifically mandated by HIPAA or other law can be agreed upon through contracts between the participating parties.	
						2) Covered entity status of the RHIO?	45 CFR 160.103 The RHIO is not a covered entity under HIPAA. See also http://www.cms.hhs.gov/apps/hipaa2decisionsupport/	
						3) Deidentified information?	HIPAA Privacy Rule may be an obstacle for the covered entities (not RHIO, because we assume it is not a covered entity). 45 CFR § 164. CE may disclose deidentified information to the RHIO without patient authorization 45 CFR § 164.514. However, if disease management is the purpose of the disclosures as stated in the scenario, it is likely that the information will not be deidentified. If PHI or IIHI is disclosed to the RHIO by a CE, either a BA agreement or patient authorization is required.	
						4) Is the RHIO required to sign a Business Associates agreement?	45 CFR 160.103. Yes, the RHIO most likely would be conducting "data analysis" on behalf of the participating organizations.	
						5) Consistent procedures for de-identifying data	If deidentifying, covered entities would be required to remove all information from protected health information under HIPAA that is individually identifiable health information. Identifiable refers not only to data that is explicitly linked to a particular individual (that's identified information). It also includes health information with data items which reasonably could be expected to allow individual identification. 45 CFR 164.502 and 514	
						6) Is there sufficient specificity in the patient authorization?	45 CFR 164.502(e), 45 CFR 164.508. Because the RHIO is not a covered entity or an organized health care arrangement, patient authorization meeting HIPAA requirements would be required for a participant organization disclosure to the RHIO unless the information is used and disclosed pursuant to a HIPAA compliant business associate agreement. If no BA agreement is in place, patient authorization to use and disclose would be a significant barrier.	

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
7	Research Data Use Scenario	Release of information to researchers	1. The Health Insurance Portability and Accountability Act (HIPAA) Standards for the Privacy of Individually Identifiable Health Information (the Privacy Rule) require that a prospective research subject execute a written authorization to allow an investigator to use a subject's individually identifiable health information for research purposes, including incorporating the information into an electronic database for the study. In the case of minors, a parent or legal guardian must complete the HIPAA authorization on the child's behalf. The authorization must describe, with specificity, what the health information will be used for, who will have access to the information (including, for example, the principal, the co-investigator, the institutional review board (IRB) reviewing the research, the sponsor, and federal oversight agencies such as the Food and Drug Administration), how long the information will be used, and that the subject's health information will be placed in a database for the project.	1,2,4,5,6,7,8	Hospitals, Clinicians, Researchers, Consumers, Research Subjects, Laboratories, Government Payors and Research Sponsors, Private Payors, Corporate Research Sponsors.	1. Authorization is required from patient to use data in study	1. 45 CFR 164.508, 45 CFR 46.101, and 21 CFR 50.20. The Privacy Rule and the Common Rule generally require that a research subject execute a written authorization to allow an investigator to use a subject's individually identifiable health information for research purposes, including incorporating the information into an electronic database for the study. In the case of minors, a parent or legal guardian must complete the HIPAA authorization on the child's behalf. The authorization must describe, with specificity, what the health information will be used for, who will have access to the information (including, for example, the principal, the co-investigator, the institutional review board (IRB) reviewing the research, the sponsor, and federal oversight agencies such as the Food and Drug Administration), how long the information will be used, and that the subject's health information will be placed in a database for the project.	42 CFR Part 431 and ORC sections 5101.27 and 5101.27. If the clinical trial involves the collection of subject payment information from public assistance programs, then the specific consent requirements contained in the federal and state Medicaid regulations may also apply.
						2. Research must fall under authority of IRB	2. 45 CFR 46.103(b). The Common Rule requires that an IRB review and approve research involving the use of human subjects or individually identifiable health information.	2. If the clinical trial also involved the collection of subject payment information from public assistance programs, then the confidentiality and consent requirements contained in the federal and state Medicaid regulations would also apply.
						3. What protocols are followed by IRB?	3. 45 CFR 46.101(b). The Common Rule requires that an IRB review proposed research plans (protocols) involving the use of human subjects, unless the protocol meets the criteria for one or more of the exemptions from formal IRB review contained in the federal regulations.	
						4. There are varying consent requirements for minors/adults/guardians	45 CFR 46 Subpart D. In addition to the Privacy Rule's individual authorization requirement, the Common Rule requires that a signed consent be obtained from potential research subjects, which explains the potential benefits and risks associated with their participation in the study. The Privacy Rule allows the HIPAA authorization and consents to be combined into a single document. The Common Rule requires that children who participate in research studies provide assent, while one or both of their parents (depending on the risks involved in the study) also provide written parental permission.	Although guardians may legally provide consent for children for medically-necessary treatment, Ohio law does not specifically address the authority of guardians to provide permission for children to participate in research studies.
7	Research Data Use Scenario	Release of information to researchers through IRB		1,2,4,5,6,7,8	Hospitals, Clinicians, Consumers, Laboratories, Government, Payers	5. How to handle request from someone outside the research protocol?	45 CFR 46.101, 21 CFR 50.20, 21 CFR 50.23, 45 CFR 164.512 and Department of Health and Human Services Office for Human Research Protections. August 10, 2004 Guidance on Research Involving Coded Private Information or Biological Specimens. The HIPAA Privacy Rule requires that an authorization describe to subjects who will have access to their individual health information used in the study, as well as how long the information will be kept or used. Similarly, the Common Rule requires the IRB to approve the study methodology, including how the database will be accessed, used and secured. Both the Privacy and Common Rules, however, provide mechanisms that allow the use of study data by researchers not included in the original IRB-approved protocol and disclosed to subjects in the HIPAA authorization. Specifically, both the Privacy Rule and guidance from the federal Office of Human Research Protections allow the research data to be deidentified and provided to the postdoctoral fellow for use in a white paper not related to the original research. In order to provide individually identifiable health information to the however, the principal investigator must obtain re-consent and authorization from the subjects for use not included in the original protocol and authorization. The Rules also provide a mechanism for the investigator and fellow to formally request a waiver of individual authorization and informed consent from the IRB - if specific criteria included in the Rules are met. The federal Food and Drug Administration (FDA) Policy for the Protection of Human Subjects, however, does not generally allow waivers of informed consent. As a result, the white paper could not be used to support a new drug application submitted to the FDA.	

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
						6. How is data tracked beyond the IRB approved timeframe?	See the citations in Obstacle #5 above. If an investigator wants to extend the length of the study to collect and track personal health information beyond the time frame specified in the consent and authorization and approved by the IRB, the Privacy Rule and the Common Rules requires that subjects consent to the proposed additional use. As noted in the above question, both the Privacy Rule and Common Rule, however, allow the principal investigator to request a waiver of individual authorization and consent from subjects if the specific criteria in the Common Rule are met. Such criteria include the practicability of obtaining re-consent as well as the nature and risks and benefits associated with the proposed additional use. In this scenario, however, a waiver is unavailable, since the research involves the study of a new ADD/ADHD drug, which is regulated by the FDA. As a result, the principal and/or co-investigator will likely need to re-consent the subjects and their parents or guardians in order to collect individual health information for an additional six month period.	
						7. Can IRB authorize use of data beyond original intent?	See the citations and answer to Obstacle #5 above.	

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	LEGAL REVIEW	DOMAIN	STAKEHOLDERS	OBSTACLES	ANALYSIS	OTHER LEGAL BARRIERS
8	Law Enforcement Access Scenario	1) Prohibited release of Personal Health Information	1. To release the patient's blood alcohol test results to the police officer pursuant to HIPAA (45 CFR 164.512(f)(1)), the disclosure would have to be required by state law, or pursuant to: a court order or subpoena or summons issued by a judicial officer, grand jury request, or an administrative request (administrative subpoena, summons, authorized investigative demand) that is relevant and material to a legitimate law enforcement inquiry, specific and limited in scope and not able to be provided in a de-identified format. To be a required disclosure under state law (ORC 2317.022), the officer would have to submit a "written statement requesting the release of records" indicating that an official criminal investigation has begun regarding a person, pursuant to Ohio law.	1 - 9	Hospitals, Clinicians, Consumers, Laboratories, Payers, Government, Providers	1) Restrictions on the release of PHI	45 CFR 164.508 (a)	
		2) Authorization to release information to parents of non-minor.	2. Pursuant to HIPAA, parents not permitted to review the ER record and lab results unless patient signs authorization allowing for the disclosure 164.508(a) OR the parents have been designated by the son as his "attorney in fact" in a durable power of attorney for healthcare and he was not competent to make his own healthcare decisions. 45 CFR 164.502(g)(2). Note: Parents receipt of EOB from insurance company - EOB would only contain billing information and would not permit parents to access medial information.			2) Is an authorization required for release of information to parents?	45 CFR 164.508(a)	
						3) Law enforcement access must be limited to specific electronic record. Not authorized to view entire medical record.	See Legal Review #1	
						4) Is there a breach of confidentiality with parents?	See Legal Review #2	
			Misc: The Federal Drug and Alcohol Confidentiality Act does not apply to most general emergency room visits (42 CFR 2.12(e)(1)).					

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
9	Pharmacy Benefit Scenario A	1) Telephone call followed by fax verification	1) Authenticating physician when calling for formulary approval (45 CFR 164.312 (d))	PD 1) ORC 4729.37 and OAC 4729-5 contemplate phone and fax contacts and set forth procedure and record keeping requirements 45 CFR 164.312 requires reasonable measures to safeguard electronic transmission of PHI	Business Associate Agreement between PBM and hospital probably necessary. 45 CFR 164.502, 504. HIPAA requirement for minimum necessary. 45 CFR 164.502.	1-9	Clinicians, Payers, Clinics, Consumer, Pharmacy, Behavioral Health
			2) There may be a delay in treating the patient	42 CFR 423.566, .568, .570 and .578 require timely benefit determinations, expedited coverage decisions and exceptions.	HIPAA requirement for minimum necessary. 45 CFR 164.502.		
			3) Part D formulary	Not sure what is being asked here. Part D formulary does not appear to be an issue. Hospital is a self-insured employer.			
			4) PBM's outside state of residence	PBM has entered into a contract with an Ohio employer to provide services to Ohio residents. To the extent applicable, PBM would be subject to Ohio law. Hospital as a self-insured employer is subject to ERISA requirements concerning the proper administration of its health plan. PBM as a subcontractor of hospital should be required to follow the same ERISA rules.			
			5) Is there a pre-authorization routine to follow?	42 CFR 423.566, .568, .570 and .578 require timely benefit determinations, expedited coverage decisions and exceptions. These rules apply to prior authorization requirements.			

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
10	Pharmacy Benefit Scenario B	1) Use of a secure Virtual Private Network (VPN) with secure private mailbox	1) Business Associate agreement required to share data	Employer is a "Covered Entity" for HIPAA. 45 CFR 160.103. Business Associate Agreement between hospital and PBM is necessary. 45 CFR 164.502, 504.		1-9	Pharmacy, Consumer, Payers
		2) Procedure for storing received data	2) Does employee have to give consent?	Employee consent not necessary as this sort of business planning is included in the definition of "operations". 45 CFR 164.501			
		3) Secure FTP via VPN	3) Is the data de-identified between PBM's?	Minimum necessary standard does apply. 45 CFR 164.502 (B)			
		4) State of Ohio uses direct TLS	4) Must the data be encrypted before sharing?	A Covered Entity must implement technical policies and procedures such that only persons/programs that have access rights information can access the information. Encryption may be a part of this. 45 CFR 164.306			
			5) Provide only minimum necessary information	Minimum necessary standard does apply. 45 CFR 164.502 (B)			
			6) Report notification of data availability	Not sure what is being asked here.			
			7) Lack of virus protection from the VPN	A Covered Entity must implement technical policies and procedures to prevent, detect, contain and correct security violations. This would likely include virus protection. 45 CFR 164.308			
			8) What is the encryption standard?	A Covered Entity must implement technical policies and procedures such that only persons/programs that have access rights information can access the information. Encryption may be a part of this. 45 CFR 164.306			

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
11	Healthcare Operations and Marketing Scenario A	1) Notice of privacy practice consent	1) What level of consent is required?	This depends on the nature of ABC Health Care (the integrated health delivery system). If ABC Health Care itself is a HIPAA "covered entity" (as opposed to holding company or corporate entity that does not provide covered services), it (along with its affiliated hospitals) could be part of an organized health care arrangement (OHCA) or an affiliated covered entity (ACE) under HIPAA. In such case, the use and disclosure of PHI by ABC (as part of the OHCA or ACE) would be the same as use and disclosure of the affiliated hospitals. If ABC Health Care is not a covered entity, the communication activities must emanate from the hospital (i.e., covered entity) level. First, consider whether the critical access hospitals can disclose PHI to DEF Medical Center for DEF's "health care operations" under 45 CFR 164.506(c)(4). If the covered entities cannot share/disclose PHI, each of the hospitals must make the communications with its own patients. The definition of "marketing" under HIPAA is the key to the analysis of whether these communications are permissible under HIPAA. Under 45 CFR 164.501, "Marketing" does not include communications "(i) to describe a health-related product or service ...that is provided by...the covered entity making the communication,...or (iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual." Thus, it would appear that DEF could make the communication with all patients (assuming it properly received the PHI as part of an OHCA, ACE or for health care operations) under clause (i) above -- or each of the affiliated critical access hospitals could make the communication as a recommendation of "alternative... health care providers or settings of care" under clause (iii) above.		1-9 excluding 8	Hospital, Consumer, Clinicians
			2) Can demographic data be separated from diagnosis?	For the reasons stated above, the information does not need be separated (except to the extent required for compliance with the minimum necessary standard). In fact, OCR has indicated in its guidance that communications regarding services offered by a hospital can be targeted to patients with specific conditions. See page 71 of OCR HIPAA Privacy Guidance, December 3, 2002, p. 71 and p. 76. Also, there may be other avenues for the hospital to obtain demographic information that does not contain diagnosis information (e.g., billing records).			
			3) Should the integrated health system be identified in marketing material?	There is no HIPAA reason that ABC's name should be excluded -- as long as it is clear that the communication is coming from the appropriate covered entity.			
				Suggested Business Practices:			
				1. Decision to conduct marketing using PHI with their consumers - As discussed in the Legal Review of obstacle #1, the activities described do not meet the definition of "marketing" under HIPAA if (i) the activities meet an exception to the definition of marketing and (ii) are performed by the appropriate covered entity. Other activities that fall outside the exceptions to HIPAA's definition of "marketing" or that would be performed by entities other than the appropriate covered entity would require a HIPAA-compliant authorization from the patient. No significant barrier to implementation of EHR.			
				2. Authorization from consumer to allow IHDS to market to themselves-- As discussed above, depending on the facts of the particular situation, it may be permissible for the IHDS to perform certain activities without patient authorization. Otherwise, an authorization must be obtained or the activities undertaken by another entity. Thus, a minimal barrier may exist, but this barrier already exists (regardless of EHR implementation).			
				3. Determine mode of transferring information and type of information, i.e., identifiable or de-identified information to the marketing department. -- Again, the resolution of this issue will depend on the facts, which should be analyzed on a case-by-case basis, but (as described above) the activities described can be undertaken without de-identifying the PHI if all applicable HIPAA requirements are met (e.g., the minimum necessary standard). Thus, a minimal barrier may exist, but this barrier already exists (regardless of EHR implementation).			

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
12	Healthcare Operations and Marketing Scenario B	1) Notice of privacy practice consent	1) Can the data be sold?	Only with a legally compliant authorization. See 45 CFR 164.508		1-9 excluding 8	Hospital, Consumer, Clinicians
		2) HIPAA compliant authorization	2) Is there a patient authorization in the privacy notice?	As described below, patient authorization is not needed for the hospital to send information to its patients concerning the services available at the hospital. See 45 CFR 501 (definition of "marketing").			
		3) Registration through OB offices	3) Where is the mailing data stored and secured?	As long as within the covered entity's facilities/control - it is just like any other PHI and should be treated like other PHI (because it is PHI) -- regardless if it is on a marketing server or other location separate from the server that maintains the hospital's clinical data. If a third party is used to perform tasks related to the dissemination of the information, the hospital must enter into a HIPAA-compliant business associate agreement with such third party. PD#3 Work group did not understand this procedure.			
			4) Will marketing require MIS to generate mailing list?	This is an operational question, but we assume that some member of the hospital's workforce will need to generate a mailing list. This person will be subject to the hospital's HIPAA policies and procedures. If a third party is used to perform this task, the hospital must enter into a HIPAA-compliant business associate agreement with such third party.			
			5) Authorization of parents and or guardians if patient is a minor	Personal representatives are treated as the individual for HIPAA purposes, so whatever rights (or obligations) that exist with respect to the individual exist with respect to the personal representative. See 45 CFR 164.502(g).			
		Suggested Business Practices					
				Analysis of the Purposes:			
		1. Ask patient permission to use and sell identifiable data for marketing --As noted in the Legal Review portion of this analysis, certain activities are not considered "marketing" for HIPAA purposes if they are undertaken by the appropriate covered entity. To the extent these activities can be excluded from HIPAA's definition of "marketing," no authorization is needed. That being said, some covered entities may deem it appropriate to seek such authorization. Any sale of PHI to third party would require a HIPAA-compliant authorization. Thus, a minimal barrier may exist, but this barrier already exists (regardless of EHR		1. Providing patients with information on the hospital's new pediatric wing/services is a permissible purpose and is not considered "marketing" for HIPAA purposes. Under 164.501, "Marketing" does not include communications "(i) to describe a health-related product or service ...that is provided by...the covered entity making the communication." Based on OCR guidance, it appears that these communications can be targeted to patients of the hospital who recently gave birth. See OCR Guidance, December 3, 2002, p. 71.			
		2. Decision to conduct marketing using PHI with their consumers - As discussed in the Legal Review, the activities described do not meet the definition of "marketing" under HIPAA if (i) the activities meet an exception to the definition of marketing and (ii) are performed by the appropriate covered entity. Other activities that fall outside the exceptions to HIPAA's definition of "marketing" or that would be performed by entities other than the appropriate covered entity would require a HIPAA-compliant authorization from the patient. Thus, a minimal barrier may exist, but this barrier already exists (regardless of EHR implementation).		2. Although it is something of semantic distinction, this purposes should be permissible if the communication is sent for informational purposes rather than couched as a solicitation. The informational communication could include registration information. The analysis would be the same as purpose #1 above.			
		3. Determine mode of transferring information and type of information, i.e., identifiable or de-identified information to the marketing department. -- Again, the resolution of this issue will depend on the facts, which should be analyzed on a case-by-case basis, but (as described above) the activities described can be undertaken without de-identifying the PHI if all applicable HIPAA requirements are met (e.g., the minimum necessary standard). Thus, a minimal barrier may exist, but this barrier already exists (regardless of EHR implementation).		3. This purpose is fundraising (not marketing), and thus subject to HIPAA's fundraising rules -- i.e., the covered entity may use demographic information and dates of service - NOT other PHI. The fact that the hospital will use PHI for fundraising must be described in the covered entity's notice of privacy practices. See 45 CFR 164.514(f)			

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
				4. Selling PHI for the hospital's financial gain is permitted only if authorized by the patient with a HIPAA-compliant authorization. See 45 CFR 164.508.			
					In our group's discussions, we addressed issues related to Ohio's Medicaid Program, Jim Skidmore, Sr. Staff Attorney, Office of Legal Services, at Ohio Department of Job and Family Services provided the analysis set forth below. We believe further discussion is appropriate to determine whether the restrictions placed on ODJFS apply to those entities that contract with ODJFS (e.g., providers) and, if so, whether those restrictions are materially different than those set forth in HIPAA.		
					Essentially, the 42 CFR 431 Subpart F (Entitled Safeguarding Information on Applicants and Recipients) restricts disclosure of information to "purposes directly connected with the administration of the plan." Those are defined as establishing eligibility, determining the amount of assistance, providing services for the recipients (within the plan — which means the state plan, or the state's Medicaid program), and assisting or conducting investigations, prosecution on civil or criminal proceedings related to the administration of the program (42 CFR 431.302). The subpart requires that the agency have restrictions in place and that the restrictions apply to those to whom the information is released that requires them to be under the same standards of confidentiality as the agency itself. Thus, the hospital is under the same standards of release of the information (42 CFR 431.306). The types of information subject to the safeguards includes names and addresses, medical services, social and economic conditions, evaluations of personal information, medical data (including diagnosis and past medical history information received for verifying income eligibility, and any information regarding identity of third party resources (42 CFR 431.305). There is also a requirement similar to the HIPAA requirement that only the minimum necessary information be released if the conditions are met for such release.		
					Ohio Revised Code Section 5101.27 covers not only Medicaid but all public assistance programs and restricts the release of information to the recipient, an authorized representative, legal guardian, or the attorney of the recipient (but only if there is written authorization that complies with ORC 5101.271). 5101.27(D) permits the release of information if the recipient provides voluntary, written authorization and the release is permitted by federal law. ORC 5101.27(F) permits the release by the agency (and by extension, and through the provision in the provider agreement that subjects a provider, including a hospital, to the same confidentiality restrictions of the agency) if the release is for purposes "directly connected to the administration of or provision of medical assistance provided under a public assistance program" and the information is released to an entity subject to the standards of confidentiality comparable to those of the agency. Clearly, it all ties back to the same confidentiality standards of the agency, so whether the release is by ODJFS or the hospital, it all is covered by these regulations.		
					Ohio law also provides restrictions in the Ohio Administrative Code at Section 5101:1-37-01.1, that basically restates the restrictions in the CFR and ORC with only a bit of expansion.		
					Alternative Position		
					42 CFR 431 Subpart F does not specifically apply to health care providers. Rather, it is federal law imposing requirements on state Medicaid agencies. It requires a state Medicaid agency to adopt rules to govern its own practices to ensure that it safeguards the information of its applicants/recipients. The law cited as authority for binding providers to the state Medicaid agency standards (42 C.F.R. 431.306) provides in the pertinent subsection (b): "Access to information concerning applicants or recipients must be restricted to persons or agency representatives who are subject to standards of confidentiality that are comparable to those of the agency." (emphasis added). In the absence of specific law governing healthcare providers, this provision does not appear to provide definitive authority for the proposition that all healthcare providers must adopt separate policies for the use and disclosure of the protected health information of Medicaid applicants and recipients.		

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
13	Bioterrorism Event	1) State requirements for reporting an event	1) How is information currently transmitted?	pd #1 - Boards of health, health authorities or officials, health care providers in localities in which there are no health authorities or officials, and coroners or medical examiners shall report promptly to the department of health the existence of any of the diseases or illnesses listed in Ohio Adm Code 3701-3-02. R.C. 3701.23 The individually identifiable health information reported to public health agencies is protected (confidential and not subject to disclosure) pursuant to R.C. 3701.17. Additionally, pharmacies, poison control centers, and other health-related entities are required to inform public health agencies of unusual events. R.C. 3701.232 and 3701.201. However, during an actual terrorism event, the Federal Bureau of Investigations will be the lead agency. Presidential Decision Directives 39 (1995) and 62 (1998); see, 10 USC 382, 18 USC 175-178, 18 USC 2331-2339B. Communication and the transfer of data outside public health or hospitals will occur on an "as needed" basis and will be conducted primarily via telephone and secure facsimile transmissions. General communication and data will be via the state's Health Alert Network (HAN). Certain individuals will then have the ability to retrieve or download data from a secure, password protected website. O #1 - See above. Not a legal barrier, however, an attitudinal barrier exists. Some providers refuse to comply with state reporting requirements.	Lack of a generalized reporting immunity.	1-9	Clinicians, Physician Groups, Federal Health Facilities, Hospitals, Payers, Public Health, Community Clinics, Lab, Pharmacies, LTC, Hospice, Correctional Facilities, State Government, Trauma Centers, Poison Control Centers.
		2) Telephone call followed by fax verification	2) Knowledge of Public Health law	PD#2 - the means and timing of communicating information on reportable disease cases is set forth in Ohio Adm Code 3701-3-05 and 3701-3-08. O#2 - LWG believes all entities involved in this scenario would be aware of their reporting responsibilities. See: "Know your ABCs" - www.odh.ohio.gov/pdf/idcm/intro9.pdf ; "Infectious Disease Control Manual" - www.odh.ohio.gov/healthresources/infectiousdiseasemanual.aspx ; Relevant Administrative Code Sections - www.odh.ohio.gov/rules/final/f3701-3.aspx . Not a legal barrier			
		3) Privacy officer reviews all requests for relevance	3) Communications include telephone, fax, secure email or site visit	pd #3 - LWG not certain which privacy officers are being referenced - state level (ODH) or provider level? Obstacle 3 - procedure and timing of required communications are set forth in Ohio Adm Code 3701-3-05 and 3701-3-06 - LWG notes that HIPAA requires reasonable methods (see 45 CFR.164.306 and 312). Also, HIPAA requires an accounting of the disclosure by providers - 45 CFR 164.528. Not a legal barrier			
			4) Variations in legislation enacted vs. paper requirements	Not able to respond - not sure what this means			

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
14	Employment Information Scenario	1) Return to work in EMR electronically generated for FMLA	1) Authorization is required and patient makes the request	Yes, HIPAA-compliant patient authorization is required, which should be easily obtained because the disclosure is for the patient's benefit. See 45 CFR 164.508. PD #1 This is not necessarily a FMLA related matter. If a hospital has patient authorization there is no barrier to electronically generating a return to work document.		1-9 excluding 8	Hospital, Payer, Consumer, Payer, Clinician
		2) Requirement for PCP to authorize	2) HIPAA requirement for notice but not consent	? Work group did not understand this obstacle and PD#2. HIPAA-compliant authorization is required for a disclosure.			
		3) Transmit via secure email to secure fax receiver	3) Does care provider have right to release information to employer?	Only upon receipt of HIPAA-compliant authorization.			
			4) Emergency room issues the discharge instructions	Patient may provide employer with patient's discharge instructions. Provider may disclose discharge instructions to the employer only to the extent such disclosure is within the parameters of the authorization.			
			5) Are there restrictions on what can be shared, does minimum standard apply?	The terms of the authorization will establish the limits of the PHI that can be disclosed. The minimum necessary standard does not apply to disclosures made pursuant to an authorization (see 45 CFR 164.502(b)(2)(iii)).			
			6) Is cutting and pasting a valid legal approach?	A cut and paste approach does not pose legal problems, provided that PHI that is cut and pasted meets the requirements of the authorization. A possible exception to this is that the covered entity must ensure that metadata or hidden text is not transferred during the cut and paste process (but this is more a technical issue that would turn into a legal issue if it occurred). A practical problem may exist because it would seem more likely that PHI beyond the scope of the authorization could be inadvertently included in the disclosure if a cut and paste process is used.			
			7) Is employee protected from employment related actions?	? Work group did not understand this obstacle. The provider will disclose PHI consistent with the authorization. Any action taken pursuant to the information included in the disclosure should be an issue for the patient, not the provider.			
				Suggested Business Practices.			
				1. Determining employee agreement to release information -- This requires a HIPAA-compliant authorization, which should not create a barrier.			
				2. Determining what are the minimum necessary elements which can be legally transmitted -- as noted above, the authorization will set the parameters for the disclosure. Therefore, the minimum necessary standard does not apply and should not constitute a barrier.			
				3. Ensuring the data is secured as it is transmitted -- security measures should be taken in a manner consistent with the covered entity's HIPAA security policies and procedures (just like any other disclosure of PHI). Thus, no barrier to implementation of EHR (that is not already in existence). PD #3.			

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
					Members of our work group noted that problems that arise in this area are often due to follow-up calls from employers that seek additional information regarding the employee/patient. Providers (and their staff) need to ensure that all PHI disclosed during follow-up conversations/disclosures is within the scope of the authorization.		

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW OF BARRIERS	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
15	Public Health Active Carrier Communicable Disease Notification Scenario A	1) Right to screen for communicable disease	1) What is the state of patient's mental stability?	There are no legal barriers. Substantial state and federal legal authority exists that enable state and local health departments to screen for communicable disease, mandate treatment, provide for isolation or quarantine, share PHI with persons or entities necessary to control, prevent or mitigate disease, and utilize law enforcement to enforce. Such authority enables government to screen and manage such situations irrespective of a patient's mental health. Ohio statute specifically authorizes sharing of information with public conveyance. R.C. 339.71, et seq., See, e.g., RC 3701.06, 3701.14, 3701.17, 3701.56, 3701.81, 3707.04; and OAC 3701-03-02, 3701-03-08; section 361(b) of the Public Health Service Act, 42 USC 264(b); Executive Order 13295); 42 CFR Parts 70 and 71.		1-8	Public Health, State Government, Consumer, Law Enforcement, Clinicians
		2) State procedure for determining need to share information	2) Is the risk localized or is there a larger population of concern?	Under Ohio statutes and regulation, medical providers and labs are required to report to local and state health officials diagnoses or lab results that identify a communicable disease listed in state regulations--diseases that are considered by public health officials to represent a danger to public health. RC 3701.23 and OAC 3701-3-01 et seq.; see R.C. 339.78. ODH director has statutory discretion to share information necessary to "control, prevent or mitigate disease." RC 3701.14(J); see RC 3701.17 and 339.81. ODH works with other state health departments and the Centers for Disease Control and Prevention, with the latter's authority at 42 USC 264 et seq. and 42 CFR Parts 70 and 71. No legal barrier: federal and state statutes and regulations enable governmental response to be appropriate to the size of the risk. There are no obstacles other than risk for inappropriate response by public or private parties.			
		3) Procedures for acknowledging sensitive information	3) What are the legal rights of the State?	see answer to #2. HIPAA and state law limit disclosure of personal health information (see R.C. 3701.17 and 339.81; OAC 3701-3-08, although exceptions exist to enable public health officials to "control, prevent or mitigate disease". RC 3701.14(J); see RC 3701.17(B), 339.80, and 339.81.) There are no obstacles other than potential for human error.			
				No legal barrier: state and federal laws are compatible, and state and federal public health officials have substantial experience working together to address communicable disease. Federal government has authority to "take such measures...as [CDC] deems reasonably necessary." 42 CFR 70.2			
			4) Is a telephone conversation an acceptable form of notice?	Initial reporting of disease by providers requires use of form: RC 3701.23(D) and 339.78; OAC 3701-3-02: State is specific as the means of provider communication (see OAC 3701-3-05); however, state and federal law is not known to mandate means of communication among governmental entities. The practice of exchanging information between local, state and federal officials involves use of telephone, fax, and e-mail.			
			5) What rights does patient have when there is a threat to the health and safety of the community?	No legal barrier, although Ohio statute and regulations do not appear to provide a specific process--other than through habeas corpus writ--for a person subject to an isolation or quarantine order to appeal the order. A person with a communicable disease can refuse treatment but the state police power will enable forced isolation of the individual. See RC 339.89 (specifically as to TB), 3707.09, 3701.13, 3701.16; see 1932 OAG 4641 regarding habeas corpus.			

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
16	Public Health Newborn Screening Scenario B	1) Procedure for Physician Authorization on IVR	1) Can the newborns data be sent electronically?	ODH does not use IVR because it cannot verify the caller (the person or entity). As the official testing laboratory for Ohio, ODH receives actual blood spots from providers and then faxes results of screenings to the submitting providers. To ensure accurate communication and given the insecurity of email, ODH maintains a self-identified facsimile number for every provider. ODH puts responsibility for security of faxed information on the provider receiving the fax. The only alternative would be for each provider to own a mass spectrometer (the device needed for the testing) and ODH would only function as a results repository – could only have a completely electronic exchange of samples and results if every provider had the machine - defeats purpose of state lab doing the testing.		1-9	Hospital, Laboratory, Consumer, State Government, Payer
		2) Storage and security of minor patient records	2) How will the patient record be tracked over time?	Newborn screening statute renders the information confidential – results are sent to birth hospital and to POR. ODH security is tighter than HIPAA security rule because of terrorism issues. No state law mandates a tracking disclosure of PHI or authorizes a public health authority (Ohio Department of Health) to track the child over time. This is a potential privacy concern barrier because no law governs. ODH does some follow-up to make sure the child is referred to a care provider but management of care is left to care providers. Bureau of Children with Medical Handicaps (BCMh) provides benefits (payments) for services = supplemental insurance.			
			3) What are the state's requirement for storing the data?	ODH retains results for 21 years.			
			4) Can role based access be implemented across multiple entities?	ODH already uses role based access. The program does not apply to multiple entities. It is an ODH internal data base			
		LWG Description of Ohio law and procedures currently in place		<i>O.R.C. § 3701.501 et al. Testing of Newborns.</i>			
				<i>O.R.C. § 3701.501(A).</i> Requires all newborn children to be screened for the presence of the genetic, endocrine, and metabolic disorders specified in rules.			
				<i>O.R.C. § 3701.501(D)(6).</i> Requires the rules adopted by the Director of Health to include standards and procedures for “referring children who receive abnormal screening or rescreening results to providers of follow-up services”			
				<i>O.A.C. § 3701-55-03 Public health laboratory responsibilities.</i>			
				<i>O.A.C. § 3701-55-03(D).</i> Requires the public health laboratory to keep a record on each newborn child screened by the laboratory for no less than twenty-one years.			

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
				<i>O.A.C. § 3701-55-08 Procedure following repeat screening or diagnostic testing.</i>			
				<i>O.A.C. § 3701-55-08(A).</i> Provides that when a newborn tests positive, the attending physician or birth facility will refer the child for further diagnostic testing, follow-up and management.			
				<i>O.A.C. § 3701-55-08(B).</i> The physician to whom the child is referred must notify the director of the Department of Health of the results and disposition of the child within 30 days.			
				<i>O.A.C. § 3701-55-08(C).</i> The Director of ODH may share newborn screening information with programs with in ODH and entities under grant/contract with ODH to assist in locating a newborn child and otherwise carry out the functions and responsibilities of the Director and ODH.			
				<i>O.A.C. § 3701-36-08. Genetic disease control.</i>			
				<i>O.A.C. § 3701-36-08(B)(2).</i> Requires each local Department of Health to maintain a record of individuals with a confirmed diagnosis of genetic disease.			
		LWG HIPAA analysis		<i>45 C.F.R. § 164.512(a) Standard: uses and disclosure required by law.</i> A CE may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law.			
				The uses and disclosures related to relaying the results of the testing and notification of state programs are mandated by the newborn screening statutes and regulations in addition to being for treatment purposes.			
				<i>45 C.F.R. § 164.512(b) Standard: uses and disclosures for public health activities.</i> A CE may disclose PHI to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability.			

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
17	Public Health Homeless Shelters Scenario C	1) Obtaining consent to treat mental health patients	1) Data can only be sent within the restrictions imposed for mental health patients	Obstacle #1: Scenario does not address mental health patients but does address a drug and alcohol patient. The primary care physician can share info with the drug clinic as two providers for the purpose of treatment under HIPAA (164.506(c)(2)). Ohio law is not a barrier to this disclosure.		1-9	Consumer, Clinician, Behavior Health, Community Clinics and Health Centers
		2) Procedure for billing government entity	2) Does a personal representative have the same rights to privacy as the individual being treated?	Obstacle #2 A personal representative of an individual pursuant to HIPAA, is to be treated as the individual with respect to PHI. 45 CFR 164.502(g)	The shelter is not a covered entity and could share its info with the relative. The drug program could not share any info without an authorization (42 CFR § 2.33, OAC 3793:2-1-06(H)). The PCP could share info with the relative if the patient signs an authorization allowing for the disclosure (164.508(a)) OR the relative has been designated by the patient as his "attorney in fact" in a durable power of attorney for healthcare and he was not competent to make his own healthcare decisions. 45 CFR 164.502(g)(2).		Consumer, Clinician, Behavior Health, Community Clinics and Health Centers, Government
		3) Policy not to release medical information vs. State law	3) Can the minimum necessary rule apply to county for payment?	Obstacle #3 HIPAA requires covered entities to limit PHI being used, disclosed, or requested to the minimum necessary. 45 CFR 164.502(b)(1). 42 CFR Part 2 requires any disclosure to be limited to that information which is necessary to carry out the purpose of the disclosure. 42 CFR 2.13(a)	Based upon the facts presented, there may be an additional potential legal obstacle. The facts presented do not indicate whether the homeless man receives public assistance. The fact that the man has a primary provider and the statement that the man is to be sent to a hospital-affiliated drug treatment facility "for his addiction under a county program" lends credence that the homeless man may be receiving public assistance, which may include a public medical assistance program or Medicaid coverage for medical assistance. If the homeless man does receive a medical benefit through a public medical assistance program the confidentiality statutes may restrict the release of information. ORC 5101.27 addresses all public assistance, including Medicaid. If the homeless man receives, or is eligible for, Medicaid, confidentiality of information is also subject to 42 CFR 431 Subpart F and OAC 5101:1-37-01.1.		Consumer, Clinician, Behavior Health, Community Clinics and Health Centers
			4) Is the shelter considered a covered entity?	Obstacle #4 Shelter does not appear to be a covered entity as it is not a health plan, clearinghouse or provider pursuant to 45 CFR 160.103.			Consumer, Clinician, Behavior Health, County Shelter
			5) Should the shelter be held to the HIPAA requirements for privacy and security?	Obstacle #5 Privacy and security requirement would not apply. The shelter would have to adhere to privacy and security requirements included in any QSO/BAA that they would have with the covered entity.			Consumer, County Shelter
				Procedure #1: Client authorization is needed to treat drug and alcohol patients pursuant to ohio law and the federal drug and alcohol confidentiality law (42 CFR § 2.33; OAC 3793:2-1-06(D)(1)(a)).			
				Procedure #2 HIPAA does not require programs to get consent before disclosing information for the purpose of payment. Proper consent pursuant to 42 CFR 2.31(a) should be used to allow disclosure for billing to comply with 42 CFR part 2. The drug clinic would need a client authorization (42 CFR § 2.33; OAC 3793:2-1-06(D)(1)(a)) or QSO/BAA with the county to share info for the purposes of program reimbursement (42 CFR § 2.12 (c)(4)) pursuant to the federal drug and alcohol confidentiality law and Ohio law. Assuming that the county shelter needs the info from the clinic for reimbursement purposes, a QSO/BAA would need to be in place in the absence of an authorization (42 CFR § 2.12 (c)(4)) pursuant to the federal drug and alcohol confidentiality law.			
				Procedure #3 If state law is stricter than the agency's policy, state law must be followed with respect to the release of information.			

HISPC Legal Work Group Modified Worksheet

#	SCENARIOS	PROCEDURE DESCRIPTION	OBSTACLES	LEGAL REVIEW	OTHER LEGAL BARRIERS	DOMAIN	STAKEHOLDERS
18	Health Oversight Legal Compliance/Government Accountability	1) Provide the minimum necessary information for request. See Obstacle #6, 42 CFR Section 164.502.	1) There is a lack of a common format	1) This is a barrier but not a legal barrier as there is a lack of common formats and identifiers that would allow for meaningful exchange of information among agencies and between several states.		1-9	Government, Consumers, Medical and Public Health Schools, Public Health Agencies
		2) Procedure to track record disclosures. See Obstacle # 6; 45 CFR Section 164.528: accounting for disclosures of protected health information	2) There are no common identifiers	2) This is a barrier but not a legal barrier; see response to Obstacle 1) above.			
		3) Memorandum of understanding with other agencies. See Obstacle #6, 45 CFR Section 164(504)(e): business associate contracts and 45 CFR Section 164.514(e)(4): data use agreement. Also, even with an MOU, federal and state Medicaid regulations will limit the purpose for disclosures of recipient	3) Lack of common data standards	3) This is a barrier but not a legal barrier as common data standards do not exist for exchange of the information pertinent to this scenario.			
			4) There is limited or little interoperability	4) This is a barrier but not a legal barrier; see response to Obstacle (1) and (3) above.			
			5) Is there a legal difference in the educational vs. medical record?	5) This is a legal barrier as the Family Educational Rights and Privacy Act (FERPA); 34 CFR Part 99, applies to educational records and the privacy protections are not entirely consistent with HIPAA. Authorization/consent will likely be required by parents for the release of the educational record. There is an exception that may or may not apply to this scenario; 34 CFR 99.31: permitted disclosures in cases of health			
			6) What rules/laws apply to disclosure of the record?	This will present a legal barrier as numerous federal and state laws will apply to the disclosure of the records. Please consider the following:			
				Federal regulations related to Medicaid. 42 CFR Part 431 Subpart F Safeguarding Information on Applicants			
				State laws and regulations restricting the release of information regarding recipients of public assistance programs including Medicaid. ORC Section 5101.27 and OAC Section 5101:1-37-01.1			
				HIPAA restrictions and requirements for uses and disclosures of protected health information:			
				45 CFR Section 164.502: general prohibition on release			
				45 CFR Sections 164.502(b) and 164.514(d)(1) and (e)(1) : minimum necessary standards and limited data set. Applicable to Procedure Description (1).			
				45 CFR Section 164.508: authorizations			
				45 CFR Section 164.512(a): uses and disclosures required by law			
				45 CFR Section 164.512(b): uses and disclosures related to a public health authority			
				45 CFR Section 164.512(i): uses and disclosures for research			
				45 CFR Section 164.514: deidentification opportunities			
				45 CFR Section 164.504(e): business associate contracts; and 45 CFR Section 164.514(e)(4): data use agreements			
				45 CFR Section 164.528: accounting of disclosures of protected health information			