State Government – Government Information Value Exchange for States (GIVES)

Tactical Implementation for HIPAA Compliance – State Governments

A White Paper Describing the Unique State Government Implementation Issues and Options for Addressing Those Issues

Version 2

Contributors: ***Rosemary B. Abell*** ***Kathleen Conner*** ***Nancy Heywood*** ***Leah Hole-Curry*** ***Mary Evenhouse*** ***Vicki Hohner*** ***Joy Pritt*** ***Karen Tomczak*** ***Sheila Zweifel***

VERSION 3 – As of 7/23/02

The following document has been prepared by GIVES for the express purpose of soliciting State Government review and input. All comments received by or before the comment closing date will be considered for inclusion in the next version of the document.

GIVES recognizes the critical importance of Industry review and input to the successful implementation of HIPAA. So please take this opportunity to participate and let your voice be heard.

Tactical Implementation for HIPAA Compliance – State Governments - White Paper

Purpose

State governments will encounter unique issues as they address the HIPAA requirements. Due to the fact that not all state governments are organized with the same structure, business relationships and business functions, there may be different options that a state can take in order to become compliant with the HIPAA standards.

This paper will identify those issues and communicate possible options when addressing certain requirements.

Scope

There is no limit to the number of issues that can be included in this paper. As issues are identified and addressed, a new version of this paper will be created.

The table below lists the state government issues currently identified. You can click either the issue number or title of the issue and a link will take you to the corresponding issue description. Options available for each issue will follow.

Issue	Title	Date	New or Revised
#1	Single vs. Multiple Covered Entities	8/14/01	New
#2	Performing a Statewide Assessment	8/14/01	New
#3	Covered Entity Status – Medicaid (Multiple roles of Medicaid)		TBD
#4	Covered Entity Status – Non-Medicaid State Government Programs (Where covered entity status appears to apply or not)	4/26/02	New
#5	Medicaid Interactions with Other State Programs – Impacts (**Note**: Any Medicaid interaction will drive the covered entity		TBD

Issue	Title	Date	New or Revised
	status of the other program, at least where Medicaid is concerned. Many state programs so small that it is not feasible or cost-effective to split into compliant/non-compliant components)		
#6	Business Compliance (Even if not legally required to comply, there are many business drivers for state government program compliance)		TBD
#7	Potential HIPAA Impacts (Vital Statistics, Public Health, Social Services - excluding Medicaid, Workers Compensation, State Employee Benefits, Corrections, Elementary Higher Education, Insurance Commissioners, State Employee Retirement, State Personnel Dept/Offices, Veteran Affairs, Employment Security, State Academic/Research Institutions, Indian Nations) Academic Medical Centers, College Health Services	4/29/02	New – partial entry
#8	Transactions – Medical Model vs. Social Service Model		TBD
#9	Voluntary Compliance with Transactions (Issues for consideration, choice of areas to comply or not)		TBD
#10	Privacy Entity Status and Implications (Considerations when making a choice of		TBD

Issue	Title	Date	New or Revised
	status)		
#11	Voluntary Compliance with Privacy (Issues for consideration, choice of areas to comply or not) Example: FERPA vs HIPAA		TBD
#12	Voluntary Compliance with Security (Issues for consideration, choice of areas to comply or not)		TBD
#13	Requirements for a Compliance Office (Implementation and beyond)	12/12/01	TBD - Karen Tomczak to initiate

Issue 1 - Single vs. Multiple Covered Entities (Statewide, Agency, Program Level)

What options can states use to declare covered entity status of the state government agencies?

Background:

Depending on the individual laws, structure, business relationships, and business functions of a state and its agencies, a determination will have to be made as to which of the various approaches available is the most appropriate.

However, all approaches should be considered to ensure that the requirements and consequences of each have been fully evaluated before making the final determination. Note that there may be different considerations for determining covered entity type under privacy vs. covered entity status for HIPAA in general.

Options:

Covered entity at the program level - Allows for autonomy within the program but creates substantial barriers to transacting or sharing information across programs within the same agency. Sharing information outside the program will now require the following:

- Trading partner or business associate agreements (depending on the use of the information)
- Security/privacy policies and procedures
- A privacy officer at the individual program level
- Establishing firewalls between the program and all other parts of the agency and external partners.

This approach lacks consistency and oversight at the agency level, thereby introducing significant agency risk. In addition, this appears to be the most expensive option, and would impose the greatest administrative and documentation burden. However, as with all approaches, if certain measures are taken risks, costs and inconsistencies can be minimized. Inconsistencies will only result if the coverage determination is left up to

each program. If the coverage determination process is centrally managed/conducted to promote consistency, then the risks are not as high. In addition, implementation costs could prove to be much lower if individual program business/IT functions are reviewed at the program level and it is determined that HIPAA compliance will not be required.

Covered entity at the sub-agency level - If the majority of the agency's business does not involve covered functions, the parts of the agency that are required to be HIPAA compliant could consider calling themselves a single covered entity. This would allow sharing across the related parts of the agency without agreements, one set of security and privacy policies and procedures, one privacy official, and a certain amount of consistency and oversight. However, this entails establishing firewalls between the programs and all other parts of the agency, although information may be regularly shared outside of the HIPAA affected programs. This approach imposes an agreement requirement when sharing outside the "covered entity" but still within the agency. In addition, this approach also lacks consistency and oversight at the agency level, introduces some agency risk, and would impose additional administrative and documentation burdens. However, taking measures as outlined in the "covered entity at the program level" approach, could also minimize risks, costs, and inconsistencies.

Covered entity at the agency level - If the majority of the agency's business is involved in covered functions, the agency could consider calling itself a single covered entity. This would allow sharing across all parts of the agency without agreements, one set of security and privacy policies and procedures, one privacy official, and agency-level consistency and oversight. This option requires the most central agency coordination and induces the least amount of agency risk. In addition, this would impose the least administrative and documentation burden. However, a great many agencies have programs and other sub-levels of the organization that operate autonomously, and imposing a new central coordination structure can be a significant political struggle and take a long time to institutionalize. There will be significant training, implementation, and monitoring costs involved to move an organization in this direction and to assure compliance. It is important to note that employees may strongly resist such a major change. These circumstances should be weighed prior to choosing this option.

Note: A major problem with this option occurs if you have non-health care programs, such as Minnesota Family Investment Program, that need to share data for operations. These programs are then at a disadvantage, as the information sharing is not allowed under "health care operations".

Covered entity applies HIPAA concepts at the agency level, but applies HIPAA requirements at the program level, or division level – There are agencies that are composed of health care and non-health care components. These agencies are known as hybrid entities, and will have certain business functions that are deemed covered under HIPAA requirements. If an agency is a hybrid entity, the covered health care components of the agency must comply with HIPAA. The other program areas could be asked to apply HIPAA concepts with an option to opt out of a particular HIPAA privacy requirement if there is a good business reason for doing so. The program opting out of the requirement should document how they will handle the requirement area (for example, based on state law). An advantage of this method is that you are documenting parts of the agency that are mandated to comply with HIPAA and thus limiting legal liability. Note that if various programs are on a shared network, access to PHI by the non-HIPAA mandated programs will have to comply with the privacy requirement of safeguarding the data, and related security provisions.

Covered entity applies at the state level across agencies – Agencies that may be subject to HIPAA, or at least those which have as their primary business covered functions as defined in HIPAA, may see benefit in declaring a single entity status to reduce barriers to sharing information and new administrative requirements to a minimum. It would also bring about a certain level of uniformity across state agencies for similar activities that the public usually expects but which rarely happen in practice. However, this is a new approach for most states, and the political barriers and concerns over control issues in this circumstance could be insurmountable. This approach also will require significant human and monetary resources for implementation and continuing compliance efforts.

Issue 2 – Performing a Statewide Assessment

What approaches can states use to determine applicability of covered entity status for state government agencies?

Background:

With the diverse business operations structured under a state department, it is important to review each department's business functions and programs. Using this information, a determination can be made if all or part of the department or agency within a department is one of the three covered entities (provider, payer, clearinghouse). This process is important to ensure that all departments know if they are or are not covered by the HIPAA regulations and to what extent.

A department may have areas that act as a plan, and those that act as a provider. In addition, if the department is a hybrid department, there may be program areas that act as a business associate of the health care component of the entity, or even a business associate of another covered entity. These program areas will also need to plan for compliance with HIPAA requirements.

Options:

Department documents their business operations and process: Each department completes a business assessment outlining the specific operations and processes. Senior management and legal staff evaluate the assessment report to determine if the department is a covered entity.

Alternatively, if you have required your privacy official to be a licensed attorney, that person could meet with program areas to determine whether an area is a covered entity, or a health care component of a covered entity. The determination should be shared with the privacy work group – if the agency is fortunate enough to have formed this valuable work group. The determination would then be reviewed by senior management for approval. Under this option, each department is responsible for their own assessment and creation of a compliance plan. At a minimum, state agencies should informally meet to share compliance tools, reach consensus on a comparison of HIPAA requirements to state laws that affect multiple departments, and share creative resolution to compliance challenges. This is imperative if various state departments supervise local units of government that work together to provide efficient local services delivery.

Statewide Assessment: It is highly recommended that initial assessments be planned and organized at an enterprise (i.e., statewide) level. A statewide assessment team should be formed that has the business/technical skills and background necessary to conduct such an assessment. Required are strong business analysis and written/oral communication skills as well as a technology and health care background.

Once formed, the first tasks of the statewide assessment team should be to develop a strategic plan and detailed work plan for conducting the assessment. The primary objective of a first-level assessment is to determine which agencies are impacted, which are potentially impacted, and which have no impact. The assessment questionnaire developed to accomplish this objective would include appropriate high-level questions to determine whether the agency is a covered, non-covered, potentially covered (needs further review), or hybrid entity. In order to conduct an appropriate assessment, all management that directly reports to the agency head must complete the questionnaire process. This is critical, because many state agencies will have a mix of covered and non-covered functions.

A second-level assessment will be required for the divisions within an agency that have not been categorized as non-covered during the first-level assessment. The second level assessment should assess related systems and business functions in regards to the HIPAA regulations to determine the level of impact, scope of remediation efforts (i.e., both business and technical considerations), and projected costs. It is critical that the appropriate legal reviews are done at completion of each stage to ensure that the assessment team results

have been scrutinized based on legal criteria and interpretation of the regulations. For example, a legal opinion is needed to ensure that the appropriate level within the government organization has been identified as the entity. An entity under HIPAA should be at the appropriate legal entity level within the state's organization. In addition, a legal opinion should be obtained from attorneys that understand the business functions of the assessed area and who have the authority to attest to whether the classification of covered or non-covered is consistent between regulations (inclusion or exclusion) and business functions of the agency. Typically, this level of expertise is available within the state's Attorney General's Office.

Assessment results should be reviewed and signed by the appropriate legal representation, as well as agency heads. It is critical that all documentation be maintained in order to provide proof that due diligence has been accomplished. Finally, the results of a statewide assessment should be organized into a strategic plan for the state to reach and maintain HIPAA compliance.

Some of the key steps in the statewide assessment process, deliverables, and considerations are listed below:

- Educate statewide management and staff about HIPAA before conducting the first level assessment so that they will understand why the assessment is needed.
- Identify and document all requirements outlined in the HIPAA regulations that relate to state agencies.
- Develop assessment tools/questionnaires.
- Conduct an assessment of the state's existing administrative processes, policies and information technology systems that relate to the requirements of HIPAA. This will require a combination of face-to-face interviews and automated questionnaires.
- Compile and analyze all assessment data.
- Provide assessment documentation for each state agency that includes the following:
  - A statement as to whether the agency is a covered entity, a non-covered entity, or a hybrid entity along with an explanation of how this was determined.
  - For those agencies that are covered, the assessment document should outline which systems, administrative processes, and policies need to be enhanced or modified. Cross-references to regulations should also be provided.
  - Narratives defining why the agency needs to comply.
  - A list of all business associates and trading partners (internal and external to each agency) should also be included.
  - Detailed documentation needs to be provided for those areas that were identified "as the make it or break it areas" for determining coverage status. This information may be needed later to justify decisions made and to prevent re-work if these areas are identified later as potential issues.
  - Detailed documentation of the scope and steps taken during the assessment should be provided.
  - Ensure that appropriate steps are taken to archive all information gathered during the assessment process.
- Provide a detailed cost and cash flow analysis for each state agency subject to compliance. This analysis should include personnel requirements; information technology hardware, software and infrastructure requirements; physical/structural requirements; and all other start-up/operational expenses needed to implement HIPAA requirements. Analysis should be provided by fiscal year and cost estimates will need to be categorized as defined by the state's accounting system/process.
- Provide timelines for implementing all HIPAA administrative, policy, and technology requirements. This would include a timeline for each agency as well as an overall timeline.
- Communicate and coordinate formal approval by each agency for all deliverables.
- Provide a recommendation on whether a statewide PMO office should be established. Recommendation should include functions of the PMO; personnel requirements; information technology hardware, software, and infrastructure requirements; and all other start-up/operational expenses. Budget/cost analysis should be provided by fiscal year and cost estimates will need to be categorized as defined by the state's accounting system/process. Cost savings that could be realized from establishing statewide PMO should also be identified.

- Develop a strategic plan for HIPAA compliance. This plan should include deliverables, recommended next steps, project phases, centralized vs. de-centralized recommendations, enterprise recommendations, assumptions, risks, budgetary requirements, and timelines.

Issue 4 – Covered Entity Status - Non-Medicaid State Government Programs

How the HIPAA Administrative Simplification law applies to a health care organization is not a clear-cut as there are options and ambiguities inherent in the intent and language of the regulations. This section lays out the key issues as they apply to public organizations that include programs whose "health plan" or "health care provider" status is at issue.

Background:

The mandates of HIPAA apply only to "covered entities" and their business associates, so it is critical to ascertain covered entity status first, before determining the impact of HIPAA. Entities who are not "covered entities" may voluntarily choose to or need to comply with HIPAA mandates in order to meet continuing business needs, adjust to data flow changes, or for other reasons. The distinction between mandatory and voluntary compliance, even if the impact is similar, is very important because "voluntary entities" are not subject to DHHS oversight and can choose to implement some, but not all, mandates. Equally critical is documentation of the analysis each entity goes through in deciding whether it is a covered entity and the results of the analysis. Voluntary compliance issues are discussed in later sections of this document.

This section explains the regulatory criteria for determining whether an entity is a covered entity or business associate. Further, this section identifies ambiguities regarding application of the criteria, explains implications, and sets forth risk factors to utilize in making decisions related to coverage.

Covered Entities:

The covered entities regulated by HIPAA are: health plans, health care providers, and health care clearinghouses. Additionally, HIPAA is applicable to any "business associate" who performs a service or covered function on behalf of the covered entity, so simply sub-contracting out does not change an entities' status nor meet compliance.

Generally, a health plan is any group that provides or pays the cost of medical care, or one of a dozen specifically named health plans including Medicaid and the State Children's Health Insurance Program.

Health care providers are defined as any group or individual that provides health care and conducts named transactions electronically. Health care is very broadly defined to include care, service or supplies related to the health of an individual, including preventive, diagnostic, maintenance, palliative care, counseling, assessment or procedure with respect to physical or mental condition, or functional status, or affecting the structure or function of the body. The full regulatory definitions are contained in the glossary.

Finally, a health care clearinghouse takes data from one entity, converts or translates the data to a new format, and sends it to another entity. A business associate is a program or organization that performs services on behalf of the covered entity. The purpose of regulating business associate relationships is so that an entity cannot avoid HIPAA regulation by outsourcing impacted business functions and to provide continuity for privacy protection.

While covered entity status is easily discerned in some cases (such as named health plans like Medicaid or providers such as public hospitals), there are gray areas that are the result of (1) the apparently conflicting requirements in the regulation's summary and the regulation itself; and (2) difficulties in applying the HIPAA definitions to the sometimes unique organizational structure and functions of government agencies and programs such as social services, public health, corrections and rehabilitation, student health centers and

atypical health related services or programs. For public agencies, this is perhaps the most difficult exercise of the HIPAA assessment and may need to be reviewed a number of times as:

- New or additional information is compiled about business practices or evolving organizational structure
- System interfaces are fully defined
- Trading or business partner relationships and expectations are identified
- HHS releases new interpretations about the applicability of the regulations.

For government agencies that have multiple programs[1] or purposes, both the status of the overall agency and the status of individual programs within the agency must be identified.

Creating or Using a Decision Tree

The criteria set forth in the regulation can be used to determine entity status. A resource that walks through the decision criteria is the CMS White Paper "Are you a Covered Entity?" http://www.hcfa.gov/medicaid/hipaa/adminsim/vol2map1.pdf. The outcome leads to findings as to whether a program is defined as, or performs functions of, a health plan, health care provider, clearinghouse, or business associate.

Consideration of potential covered entity status begins by asking whether the entity is a "named" (Medicaid, etc.) or "by function" health plan listed under Section 160.103. Health plans specifically named in the regulation cannot utilize the exceptions for government-funded programs that may be available to health plans not otherwise named. If a program is not named or is not functioning as a health plan, the analysis continues with whether the program functions as a health care provider, a clearinghouse, or a business associate.

COMMENTS CONCERNING CORRECTIONAL HEALTH CARE:
The CMS article states that if your organization is specifically exempted as a health plan -- as correctional systems are in the regulations comment section -- then that is the end of the analysis. The CMS article does not contemplate that a correctional system may be covered as a health care provider that conducts covered transactions electronically.

The regulations clearly contemplate that some correctional systems may be covered. First, if the intention was to exclude all correctional systems, that could have been unequivocally stated. Instead, certain exceptions to the rules were created for correctional systems. Second, some language clearly suggests corrections may be covered. Section 164.512(k)(5)(ii) states "A covered entity that is a correctional institution …."

For correctional institutions, the California Covered Entity assessment tool posted on the HIPAA GIVES web site would be more helpful.

Covered Entity Status Ambiguity:

While the decision criteria assists generally, the complexity of States' publicly-funded health care programs does not appear to be in the minds of those who drafted HIPAA legislation, regulations, and transaction implementation guides. Medical services delivered in a social services environment, in particular, stretch the limits of the intent of the law. The tension between the law's focus on private health care models and the reality of administration of public programs, gives HIPAA compliance for the programs the appearance of forcing a square peg into a round hole. The following text sorts out the issues and ambiguities and provides a basis for social services departments' decisions in the future.

Overall Agency Status

As noted in other sections, the issues of covered entity status for multi-program agencies begin with the status of the overall agency and state approach.

[1] As noted above, "program" is used in this document in a generic sense to indicate a defined unit, section, or division of the organization.

With respect to government programs, the regulation Comments sections of the regulations expressly indicate where compliance responsibility resides. "We further clarify that, where a public program meets the definition of "health plan" the government agency that administers the program is the covered entity."[2] This helps to clarify where the actual "entity" is, but does not assist with decisions about which programs meet the definitions and what to do with programs that may not meet the definitions if they are contained in the same agency.

We highly recommend that whatever decisions are made at agency, departmental, or state levels, there is some overall review of determinations of individual program's coverage to ensure that coverage and exception decisions are applied uniformly. An example would be what organizational level or characteristics qualify as a "program" for purposes of applying the health plan exceptions – could it be a single unit for one part of a department and an entire division in another? The overall agency purpose and level of integration are factors in determining covered status.

Once covered programs are determined, another potential departmental or agency issue arises related to the application of the privacy rule. Is the overall agency or department a single covered entity or a hybrid entity? (A hybrid entity is a "single legal entity that is a covered entity and whose covered functions are not its primary functions.") For privacy, certain organizations are allowed to formally segregate their covered entity components from their other components and only apply privacy regulations to the covered or health care component.[3]

Program Level Status Issues

Many government programs have not historically been referred to or thought of as "health plans" or "health care providers." These programs are not easily categorized using the regulatory criteria. This section sets forth the ambiguity in applying the regulation to various typical components of public health agencies. Then, the following section sets forth risk factors to consider when making its decisions about whether specific groups or programs are functioning as a covered entity.

Health Plan Ambiguities – Under HIPAA, a health plan includes specifically named programs such as Medicaid and the State Children's Health Insurance Program. The Comments to the regulation clarify that Medicaid waiver programs, including home and community based services programs are included. Additionally, any other group or individual plan that provides, or pays the cost of, medical care is included in the definition of a health plan. The regulation comments clarify this inclusive category as follows: "Therefore, to the extent that a certain benefits plan or program otherwise meets the definition of "health plan" and is not explicitly excepted, that program or plan is considered a "health plan".[4]

Similar comments also evince an intent to apply the regulation broadly: home and community based waiver services were not exempted even though it was acknowledged that the programs commonly paid for a mix of health care and non-health care services. Thus, State Medicaid Agency home and community based waiver programs, though commonly thought of as social services and not health plans, are not exempt from HIPAA coverage as a health plan.

The ambiguity, then, is the application of the regulation to components or programs within social service departments where those programs either appear not to perform a covered function or appear to meet one of the government funded health plan exceptions. Those "government funded programs" not otherwise named are (a) programs that do not have as their principal purpose the provision of or payment for the cost of health care; or (b) programs whose principal activity is the direct provision of care; or (c) programs whose principal activity is the making of grants to fund the direct provision of health care to persons are excluded.

The definition or make-up of a "government funded program" is not defined or discussed within the regulation or the Comments section. A program could conceivably be an entire agency or a single unit. This analysis is

[2] *Federal Register,* Vol. 65, p. 82578.
[3] *45 CFR* § 164.504
[4] *Federal Register,*Vol. 65, p. 82578.

further obscured by the federal "single state agency" mandate for Medicaid and the move towards integrated service delivery and systems. Finally, for the third exclusion, there is no clear definition or guidance related to a "grant to fund the direct provision of health care to persons". Some programs may not consider their payments "grants" where other programs may call a payment a "grant" where it does not fund the direct provision of health care to persons.

However, it is also acknowledged that health plans pay for non-health care services, so care must be exercised when exempting a program because it pays for some services or products that are not health care. The regulations state that not all claims submitted to health plans are for health care. Thus, it concludes, that while the health plan is covered, claims for non-emergency transportation, or carpentry services for housing modification are not regulated [because they are not for health care].[5]

Therefore, the resolution of which programs are covered depends on the application of the regulatory comments and text to the business functions of each program to and then the application of risk factors to determine the magnitude and impacts of complying or not complying with the standards. However, for health plan programs that have not historically functioned in a traditional medical model, such as the home and community health programs and other waiver programs as well, both the HIPAA terminology and business processes are foreign and not readily adaptable to the current business models.

Health Care Provider Ambiguity – Similarly, the regulation defines a health care provider as "a provider of service, a provider of medical or health, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." Health care is very broadly defined, and includes care, services, and supplies related to the health of an individual. The official comments specifically state that case management is a health care service, and agencies with home and community based waivers services are subject to the standards.[6] It also has specific exceptions to FERPA.

Clearinghouse Ambiguities – Programs that operate systems or perform functions on behalf of other programs and other entities are reviewed for HIPAA clearinghouse status. Most government programs do not meet the definition because they do not (1) convert or reformat nonstandard transactions and data elements into standard transactions and data elements (2) and receive or transmit that information to another entity. What must be considered is whether these programs *will* meet the clearinghouse definition if they support the business needs of other programs or entities that will be required use the standard transactions. Generally, remediation of program systems, even when translators are added, does not qualify the program as a clearinghouse. A health plan that uses a translator for its own payment system is not a clearinghouse.

However, ambiguity does arise where programs or programs owned systems perform services for or assist other entities (like providers). The distinction between direct data entry systems and clearinghouses becomes muddled. Government programs often create web-based entry or give software to providers so that providers can communicate directly with the government program regarding HIPAA standard transactions, such as claims or eligibility inquiries. If the providers directly enter the data into the health plan's back end system, this meets the direct data entry exception and HIPAA data content but not format must be followed.

However, if the information is not transmitted directly into the health plan's system, but instead is either placed on a server or sent first to one program, then to another program's system, the transmission does not fall within the direct data entry exception. Either the provider must comply with both the format and content of the transmission, or the system or program in the middle must convert the data into a fully compliant HIPAA transaction and send it on. If the latter option is chosen, the "middle program" is functioning as a clearinghouse. It is important to note that a system's direct data entry status is only applicable where the system into which HIPAA providers enters HIPAA transaction data is under the direct control of the back-end system of a single

[5] *Federal Register,* Vol. 65, p. 50316.
[6] *Federal Register,* Vol. 65, p. 50315

health plan. If a direct data entry system is outside of a single health plan's back-end system, then any HIPAA transaction entered must conform with the standard format as well as the data content.

Additional Risk Factors

This section presents risk factors faced by programs that offer social services.

Single Entity – While an individual unit or program area may appear to meet an exception, the overall entity functions, purpose, and mandates may control the coverage decisions as discussed above.

Integrated Services or Programs – A corollary to the single entity issue is the fact that many programs are inter-related. In addition, some programs commingle funding sources, some of which are Medicaid funds, named in HIPAA as a health plan. Many social and health service organizations are moving towards an integrated service delivery where program cooperation is critical and program boundaries become less distinct. Determinations of health plan status must factor in the extent of these overlaps especially where programs are classified differently simply because of different funding streams, system use, or business functionality.

"Medical" vs. "Social" Model – While not necessarily a "risk" factor, the modality of business is an important issue to consider in determining both coverage and extent of change required. HIPAA regulations and the Implementation Guides are based on, and describe, business-to-business relationships and transactions occurring in the medical community such as hospitals, physician offices, HMOs, and insurance plans. However, HIPAA's application is much broader than this traditional medical community (e.g., applies to atypical providers such as case management and home health as well as Medicaid and other unique government programs). Therefore, even though atypical health groups did not participate in setting the standards, and thus some business needs and processes may not be addressed by the regulation, these groups are covered entities and must seek to adapt to the standards and/or work with the designated standards maintenance organizations and HHS to get unique business needs met.

Medicaid Management Information System (MMIS) Requirements – Medicaid agencies are mandated to support an MMIS that is capable of processing all supported transactions in accordance with HIPAA for services covered under the state plan. These requirements are stated in 42 USC 1396(b), 42 CFR part 443, and the Medicaid Manual Part 11. Given that the MMIS is capable of supporting, either manually or automatically, all eight transactions covered by HIPAA, and the MMIS is required to be capable of processing transactions for all Medicaid services, it is possible to conclude that the MMIS must be capable of supporting all eight HIPAA compliant transactions for all Medicaid services, not merely traditional medical services. Although waivers have been granted to have some Medicaid transactions processed in conceptually equivalent systems, any determination about which standard transactions DHS programs must support should factor in the MMIS requirements.

Same or Similar Population and Services – Even where programs themselves are not integrated, programs may serve similar populations, and provide or pay for similar services. However, due to its funding source, one program may be clearly covered whereas others are not. Often client eligibility for these programs may fluctuate based on health status or income. Justifying different client treatment or maintaining separate business processes is difficult, e.g., protecting a patient's health information in one program but not in another.

Trading Partner Expectations – Trading partners can request or require HIPAA compliance as a condition of a continuing relationship. If a program's trading partner is required to change under HIPAA, the risk that this partner will require the program to communicate using HIPAA standards is higher. Programs that are HIPAA-defined health plans must conduct a HIPAA transaction if requested to by any entity, with the caveats stated. Programs that are clearinghouses or providers, if they wish to do business with their trading partners, will have strong business reasons to accommodate requests to conduct HIPAA transactions. Therefore, any consideration of a program's compliance risk should evaluate the likelihood that its trading partners will be using HIPAA transactions with other payers or providers.

APPLICATION

Programs considering coverage must identify current business functions, processes, funding sources, and primary business partners. Then, the program can apply the Covered Entity Decision Criteria tests to the program, and finally analyze risks associated with any "gray area" programs.

Issue 7 – Potential HIPAA Impacts – Non-Medicaid State Agencies

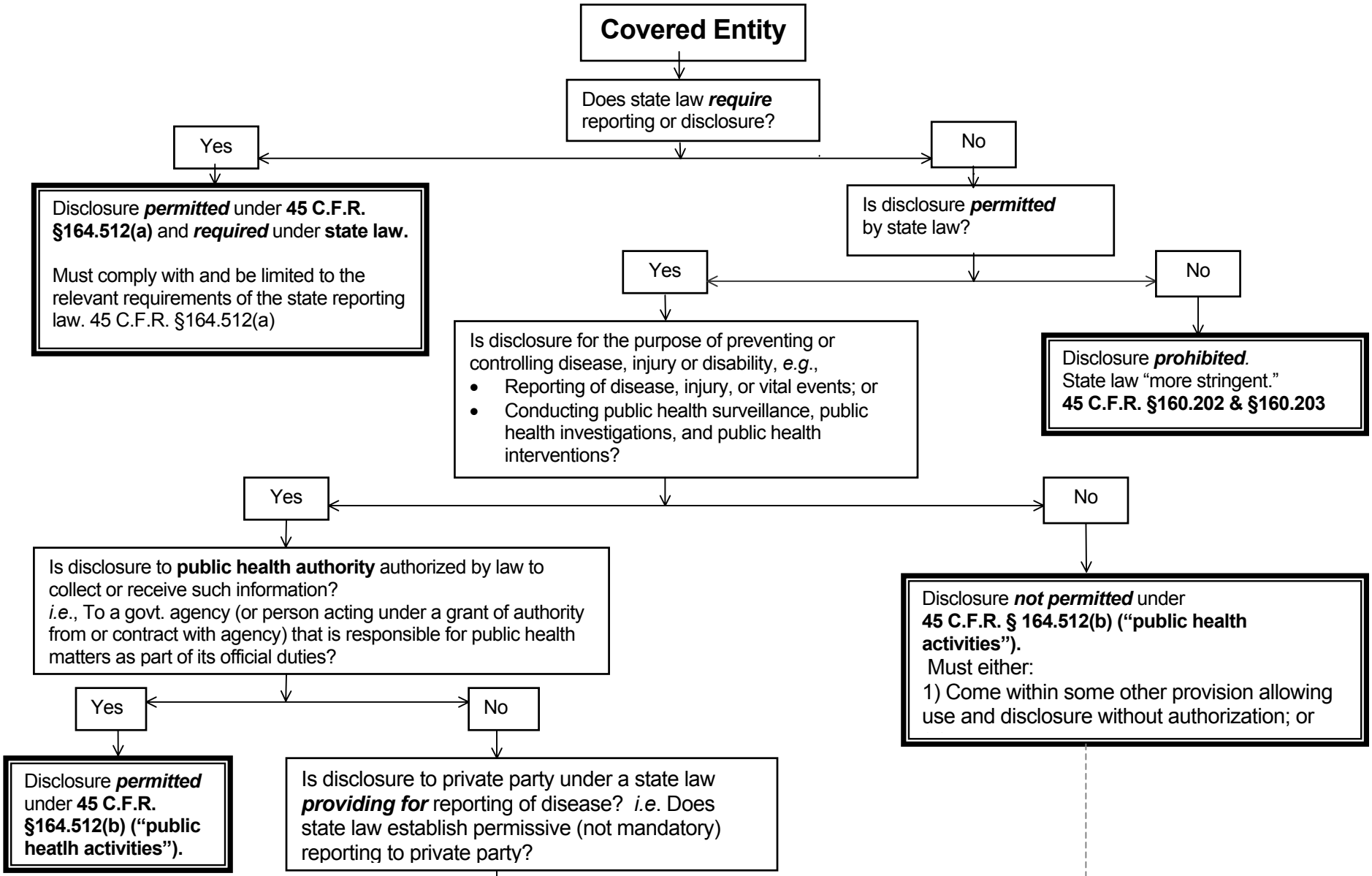
Additional non-Medicaid state agencies can be added to this issue.

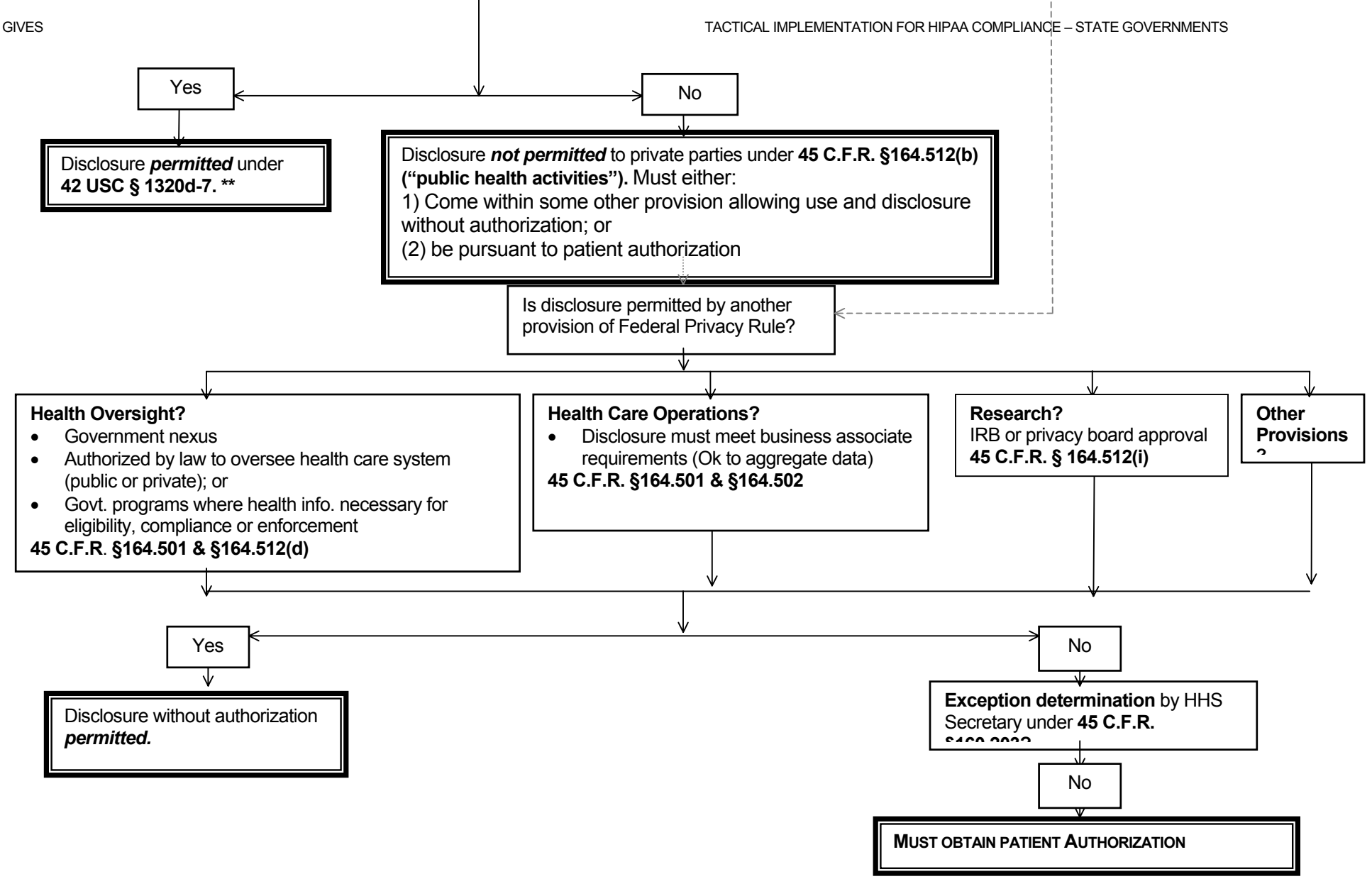
Background:

Options:

The next page contains a flow chart for determining if the HIPAA Privacy Rule permits a covered entity to disclose health information without patient authorization for Public Health purposes. The chart was developed by Joy Pritt of the Health Privacy Project in February 2002.

Does the Federal Health Privacy Rule Permit a Covered Entity to Disclose Health Information *Without* Patient Authorization for Public Health Purposes? *





* This flowchart does not address the Fed. Health Privacy Rules "public health" provisions concerning disclosures related to child abuse or neglect or that are permitted by the Food and Drug Act.

** Because the state law "provides for reporting" for public health purposes, the public health carve out from the general preemption provisions of HIPAA would apply. *See* 42 U.S. C. §1320d-7 .

End of Document