

HIPAA Compliance Project Status Report

September 13, 2002

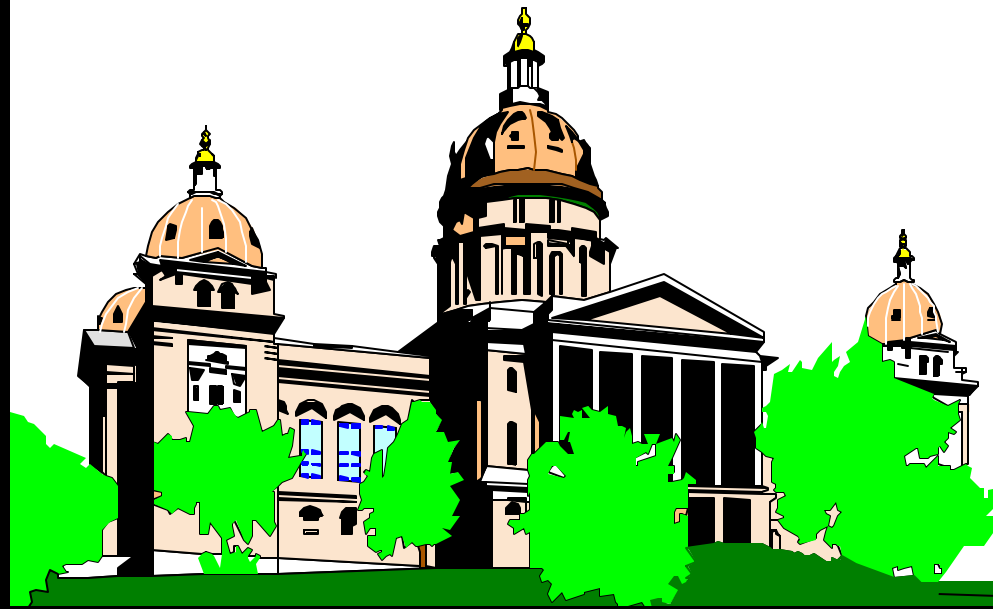
Prepared by:

Tom R. Shepherd

Enterprise HIPAA Project Administrator

Information Technology Department

State of Iowa



IOWA

State Of Iowa
HIPAA Compliance Project Status Report
September 13, 2002

Table of Contents

	<u>Page</u>
State Of Iowa HIPAA Compliance Project – Executive Summary	3
What Does HIPAA Mean for the State of Iowa as an Employer?.....	5
Implementing HIPAA.....	6
The August 14, 2002 HIPAA Final Privacy Rule Changes	7
Are There Other Laws Or Developments To Be Considered?.....	7
Appendix A. State of Iowa Executive Branch Agencies with Divisions or Programs that are Classified as HIPAA-Covered Entities.....	8
Appendix B. State of Iowa Executive Branch Agencies with Only Business Associate Status.....	15
Appendix C. The Family Medical Leave Act (FMLA) and Medical Privacy Issues for the State of Iowa as an Employer	17
Appendix D. State of Iowa Enterprise HIPAA Project Office Contacts	19

State Of Iowa HIPAA Compliance – Executive Summary

HIPAA Covered Entity Status - An initial review of all executive branch agencies has been completed with regard to their status as a HIPAA “covered entity”. HIPAA covered entities are typically healthcare payers (e.g. insurers, Medicaid) or healthcare providers (e.g. hospitals, clinics, pharmacies, and healthcare professionals). The review determined that eight state agencies have divisions or programs that are HIPAA covered entities. They are:

- Department for the Blind
- Corrections
- Education
- Human Services
- Personnel
- Public Health
- Public Safety
- Veterans Affairs/Iowa Veterans Home

Agencies used a questionnaire distributed by the Enterprise HIPAA Project Office to determine covered entity status. In some cases, questions were referred to legal counsel for clarification. A more detailed explanation for each of the agencies listed above can be found in [Appendix A](#).

For covered entities that deal with medical claims (healthcare providers submitting medical claims for payment or healthcare payers processing claims for payment), the next major HIPAA deadline is the requirement for complying with the implementation of standardized, HIPAA mandated medical claims transaction identifiers and codes. HIPAA requires that all covered entities must begin using the standard transactions and code sets by October 15, 2002 or file a request for a 1 year extension of this requirement by that date. It is essential that all agencies subject to the transaction and code set requirements file the extension request in a timely manner. The Enterprise HIPAA Project Office is tracking the extension requests and will ensure that all required extensions are filed prior to the deadline.

Will HIPAA affect state agencies that are not considered “covered entities”? Virtually all state agencies will have some HIPAA issues in being designated as a business associate of the health insurance companies providing coverage to state employees. This will require some policy and procedural changes in the handling of employee healthcare benefits information and healthcare information related to personnel administration (fitness for duty reports, workers compensation, etc). The Enterprise HIPAA Project Office will work with the Department of Personnel in developing model HIPAA compliance policies and procedures and provide this information to state agencies. The good news here is that the final privacy rule published on August 14, 2002 extends the deadline for the implementation of business associate agreements from April, 2003 to April, 2004. A more detailed explanation of the business associate requirements can be found in [Appendix B](#).

Agency Assessment Issues Requiring Follow-up or Further Coordination:

- There are a number of employees who are not FTEs in any of state agencies reviewed, however, they are covered by the State’s health plan (e.g. employees in Community Based

Corrections, the State Fair Board, etc). Business associate agreements between the insurers and the State of Iowa will need to cover these employees.

- The Department of Public Safety has a 28E agreement in place with the Iowa Department of Personnel. Jointly, they administer the Iowa Department of Public Safety Peace Officers' Retirement, Accident, and Disability System (PORS). In carrying out the administration and operation of this system, protected healthcare information –PHI - (as defined by HIPAA) is processed. Further information is being gathered as to the duties and responsibilities of the Department of Public Safety and the Department of Personnel as it relates to the handling of PHI.
- The processing of healthcare claims (Medicaid and other insurance claims) by the Area Education Agencies and School Boards throughout the state was examined. As a healthcare provider (providing certain counseling and rehabilitation services), these agencies and boards would need to either comply with the HIPAA transactions and code sets requirements or file a request for a 1 year extension to this requirement by October 15 of this year.

Project Office Services and Coordination – The project office maintains a State of Iowa HIPAA website at <http://www.state.ia.us/government/hipaa/> . To assist the Department of Human Services with their massive HIPAA compliance requirements, the Enterprise HIPAA Compliance Project Office is developing an extensive website to facilitate internal and external communications, maintain a large document data base, and provide control and coordination services for the DHS HIPAA Compliance Project Office. Once the policies, procedures, and web services being developed are moved into a production environment, they will be maintained by the Department of Human Services.

The Enterprise HIPAA Project Office has been active in the Iowa Chapter of the Strategic National Implementation Process (SNIP) for HIPAA. The SNIP is a valuable collaboration and coordination forum for the entire healthcare industry and all levels of government in pursuing solutions to HIPAA compliance. Several SNIP member organizations have donated funds to assist with the coordination of SNIP activities. The Information Technology Department has developed and deployed a SNIP website (www.iowasnip.org) and was compensated for this development with the donated SNIP funds.

The project office has been working with the Iowa State Association of Counties (ISAC) through Deb Westvold. We have made the HIPAA Covered Entity Assessment questionnaire and the HIPAA Gap Analysis available to ISAC as well as a number of research papers developed by the project office and obtained from sources around the country.

State of Iowa - Enterprise HIPAA Compliance Project - Next Phase – The project office will be monitoring the filing of the requests for extension to the transactions and code sets deadline. Priority will be placed on assisting the HIPAA covered entities with an assessment of their current situation and the development of a gap analysis, then preparation of a project plan. The deadline for compliance with the HIPAA privacy requirements for covered entities is April 14, 2003.

What Does HIPAA Mean for the State of Iowa as an Employer?

The basic privacy principle of HIPAA is straightforward: organizations that possess personal information related to an individual's health care (or payment for health care) cannot disclose it, except in the following limited circumstances:

- to the individual;
- pursuant to a signed, dated general consent form, in order to carry out treatment, payment or health care operations;
- if not for treatment, payment or health care operations, then pursuant to a signed, dated and narrowly crafted authorization; or
- to the government (state or federal) for purposes of public health, abuse/neglect investigation, fraud prevention, etc.

The Privacy Rule requires that health benefit plans:

- absent special authorization, use and disclose protected health information ("**PHI**") only for activities permitted under the rule – chiefly activities related to treatment, payment and health care operations;
- describe in a written notice published to plan beneficiaries uses and disclosures it makes of PHI unless the plan is fully insured and the plan sponsor creates or receives only summary health and enrollment information as defined by the rule;
- enter into contracts with state agencies that create or receive PHI in the course of providing services to the plan (enrollments, changes, or terminations of healthcare coverage) that require the state agency (a business associate) to use and disclose the PHI consistent with the HIPAA rule and, among other things, make the data available to beneficiaries for copying and amendment;
- implement policies and procedures allowing beneficiaries to access and copy their PHI, request restrictions on its use, request amendments to it and request an accounting of certain types of PHI disclosures; and
- develop policies restricting agency employees from access to the PHI of others, protecting PHI with physical, technical and administrative safeguards, and limiting the type of data transmitted or received to that which is minimally necessary for the function being performed.

The rules cover personally identifiable information, where the health care data can be linked to a person's name, social security number, employee number, or other identifier. It's generally acceptable to disclose summarized or redacted data, which cannot be linked to any specific individual. But the definition of "protected health information" includes any information, in any form (electronic or otherwise), created or received by a provider, health plan, insurer, or employer, that relates to past, present, or future health care or payments. Any such information, if it can be personally identified, falls under the domain of HIPAA.

HIPAA also takes healthcare information disclosure restrictions to a new level. Many providers and insurers have routinely released a broad range of health care data in the context of any given procedure or payment issue, and most patient releases have been written to offer considerable latitude for disclosure. But HIPAA largely puts an end to the days where all medical files and payment data on a particular patient can be released without question. Organizations must now make a reasonable effort to limit the release of health information to the *minimum amount of information necessary* to accomplish the purpose at hand. This requirement does not apply to disclosures to, or requests by, health care providers for treatment purposes. Nonetheless, the “minimum necessary” disclosure requirement will force insurers and employers to revamp their systems and procedures regarding what, why, and to whom protected health information is released.

Implementing HIPAA

What steps will the State of Iowa need to take to bring state agencies into compliance with HIPAA? Some steps are required by the law, and others will be an inevitable consequence of changing the way an agencies handle health care data. In general, agencies will need to ensure that they don't access health information acquired by their employee benefit plans – especially not for employment-related purposes.

For example:

- Agencies will need to reconfigure their administrative, technical, and physical safeguards for health care data. This will include changes to information systems and the creation of a “firewall” between plan-related uses of health information and employment-related uses of such information.
- Health Plan documents will need to be amended to specify permitted uses and disclosures of health information to the employer/plan sponsor.
- Agencies designated as HIPAA covered entities will be required to assign staff to develop and implement HIPAA policies, including designating a Privacy Officer (who may or may not be a new employee) with overall responsibility for HIPAA privacy issues.
- HIPAA requires Agencies to provide ongoing training for responsible employees on appropriate uses and disclosures of protected health information and to develop sanctions for non-compliance.
- As part of the compliance program, state agencies will need to conduct a thorough baseline audit of their handling of protected health information and develop tracking mechanisms to ensure ongoing compliance.
- Agencies will need to police any “business associates” with whom they share protected health information (such as technology vendors, plan administrators, etc.) and redraft contracts to assure that third parties are in full compliance with HIPAA. This is because HIPAA makes an employer liable for the violations of its business associates if the employer is aware of the associate's wrongful disclosures.

Overall, HIPAA will result in fundamental changes – legally, operationally, and technically – in how employers with employee benefit plans handle health care data.

The August 14, 2002 HIPAA Final Privacy Rule Changes

The final privacy regulations allow covered entities an additional year to amend existing written agreements to incorporate business associate provisions. Agreements that come up for renewal, other than through an automatic renewal without negotiation, must be modified to incorporate the business associate provisions at that time. All other agreements must be modified by April 14, 2004, but HHS makes clear that covered entities still must comply by April 14, 2003 with the individual rights requirements with regard to information held by their business associates. This means that state agencies will have until April 14, 2004 to comply with certain HIPAA requirements in they perform functions that would classify them as business associates.

HHS clarifies that third parties who perform a service or function for a covered entity (such as Medicaid or a state hospital) and may inadvertently come into contact with protected health information are not business associates (e.g., janitors). HHS also clarifies that a covered entity does not need a business associate agreement with a researcher, whether the researcher is performing its own research or research on behalf of the covered entity.

HHS declines to provide a business associate certification process or to eliminate the requirement for a business associate agreement between two covered entities where the relationship otherwise meets the definition of "business associate."

Regarding liability for business associate activities, HHS provides some guidance regarding when a covered entity is considered to have knowledge of a violation by its business associate, stating that the determination is based on "common principles of law that dictate when knowledge can be attributed to a corporate entity."

Are There Other Laws Or Developments To Be Considered?

Yes. The so-called "Patients Bill of Rights" ("PBR") legislation may have an impact on the designated decision makers of plans. Employers may find it appropriate to coordinate their approach to isolating the handling of PHI with their management of the PBR risk. Also relevant are the existing Americans with Disabilities Act ("ADA") regulations governing the maintenance of separate files for the results of medical examinations conducted in the context of employment or other medical records received by the employer.

Appendix A. State of Iowa Executive Branch Agencies with Divisions or Programs that are Classified as HIPAA-Covered Entities

A **Covered Entity**, as defined by HIPAA, means:

- 1) A health plan.
- 2) A health care clearinghouse (translating medical reports into standardized claims processing formats or converting one medical claims format to another).
- 3) A health care provider (e.g. hospital, clinic, pharmacy, medical practice, physician, dentist, chiropractor, nurse, pharmacist, other healthcare practitioner, or durable medical goods provider who transmits any health information in connection with a transaction covered by HIPAA).

HIPAA mandates that each covered entity designate a HIPAA Privacy Officer and will ultimately require a HIPAA Security Officer to ensure the ongoing compliance with HIPAA requirements. There must be processes established by the covered entity to provide the following services to their clients:

- Notice of HIPAA covered entity information practices
- Client access to their healthcare records
- Right to accounting of disclosures of information by the covered entity
- Right to request amendment to healthcare records
- Right to request restriction of uses and disclosures of healthcare records
- Right to request restrictions communicating healthcare information

HIPAA covered entities are required to implement ongoing HIPAA Privacy and Security training for employees and contractors as well as establish and maintain contractual agreements with [business associates](#) (see Appendix B for additional information) and trading partners requiring ongoing compliance with the applicable HIPAA requirements.

For details on individual agencies that are designated as HIPAA covered entities, please see the chart that begins on the next page.

State Agencies With Divisions or Programs That Are HIPAA Covered Entities			
A. State Agency	D. HIPAA Covered Entity Status (Covered Entity Type, Business Associate, Trading Partner)	E. Subject to Transactions & Code Sets (TCS) Deadline?	F. Date TCS Deadline Extension Request Filed
Agency HIPAA Issues			
Blind	<input checked="" type="checkbox"/> Covered Entity <i>If Covered Entity:</i> <input checked="" type="checkbox"/> Payer <input type="checkbox"/> Provider <input checked="" type="checkbox"/> Business Associate <input type="checkbox"/> Trading Partner	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Pending
<p>The Department for the Blind pays for eye examinations and, in some cases, for eye glasses, canes, magnifiers, and other assistive devices for qualified constituents. The department currently does not receive or process payment claims in electronic form, however, it is recommended that they file for the transactions and code sets extensions as a precaution.</p>			
Corrections	<input checked="" type="checkbox"/> Covered Entity <i>If Covered Entity:</i> <input type="checkbox"/> Payer <input checked="" type="checkbox"/> Provider <input checked="" type="checkbox"/> Business Associate <input type="checkbox"/> Trading Partner	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Pending
<p>The Department of Corrections directly provides psychiatric and counseling services and performs tooth extractions. Other medical services are contracted through University of Iowa Hospitals and Clinics.</p> <p>Additionally, the HIPAA provisions for persons in correctional institutions and in psychiatric institutions for correctional purposes are different than for the general public. This will require policy and procedural changes. It provides family members (or other designees) of the inmates with certain rights and responsibilities for the control and release of protected health information (PHI) on behalf of the inmate. It also allows for the exchange of certain PHI within the correctional institution for the necessary treatment of inmates and operation of the institution without having to obtain a release from the inmate or their designee.</p> <p>Healthcare services are performed internally or under pre-existing contracts, however, it is recommended that they file for the transactions and code sets extensions as a precaution.</p>			

State Agencies With Divisions or Programs That Are HIPAA Covered Entities			
A. State Agency	D. HIPAA Covered Entity Status (Covered Entity Type, Business Associate, Trading Partner)	E. Subject to Transactions & Code Sets (TCS) Deadline?	F. Date TCS Deadline Extension Request Filed
Agency HIPAA Issues			
Education	<input checked="" type="checkbox"/> Covered Entity <i>If Covered Entity:</i> <input type="checkbox"/> Payer <input checked="" type="checkbox"/> Provider <input checked="" type="checkbox"/> Business Associate <input type="checkbox"/> Trading Partner	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	Pending
<p>The Vocational Rehabilitation Division of the Department of Education, by virtue of their training and counseling services to persons with disabilities is considered a provider under HIPAA.</p> <p>Additionally, the Area Education Agencies and school districts file Medicaid and other related medical claims on behalf of their constituents. This will require the AEA's and the school districts to file the claims using the HIPAA mandated medical transactions and code sets. The project office is working with the department in determining the most effective way to file for the transactions and code sets extensions for AEA's and school boards.</p> <p>The project office will be meeting with representatives from the Department of Education within the next two weeks to determine the scope and requirements for filing one extension request on behalf of all AEA's and school boards and filing a combined compliance plan. The project office will be contacting the HHS regional office in Kansas City to inquire as to the legitimacy of such a blanket filing. HHS has indicated that each covered entity must file for the extension. They do allow large entities (the Iowa Department of Human Services, for example) to file as one hybrid organization (with some divisions or programs that are covered entities and some that are not covered). There are questions as to what authority or control the hybrid entity must have over the covered divisions or programs in order to allow for such a single, umbrella filing.</p>			

State Agencies With Divisions or Programs That Are HIPAA Covered Entities			
A. State Agency	D. HIPAA Covered Entity Status (Covered Entity Type, Business Associate, Trading Partner)	E. Subject to Transactions & Code Sets (TCS) Deadline?	F. Date TCS Deadline Extension Request Filed
Agency HIPAA Issues			
Human Services	<input checked="" type="checkbox"/> Covered Entity <i>If Covered Entity:</i> <input checked="" type="checkbox"/> Payer <input checked="" type="checkbox"/> Provider <input checked="" type="checkbox"/> Business Associate <input type="checkbox"/> Trading Partner	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	August 23, 2002
<p>Due to the extensive HIPAA requirements for the Department of Human Services, they have formed a HIPAA Compliance Project Office with one dedicated FTE and a HIPAA related job assignments for a diverse group of employees within DHS.</p> <p>The Department of Human Services functions as a payer in its role as the state Medicaid Administrator. As such, it must use the HIPAA mandated transactions and code sets for processing payments for medical claims.</p> <p>The department assumes the role of provider by operating the state mental health institutions. This will require extensive changes in policies and procedures.</p> <p>The department filed a single request for extension of the transactions and code sets deadline for the whole department. The HIPAA compliance plan filed with the request for extension addressed Medicaid and Mental Health Institutions separately.</p>			

State Agencies With Divisions or Programs That Are HIPAA Covered Entities			
A. State Agency	D. HIPAA Covered Entity Status (Covered Entity Type, Business Associate, Trading Partner)	E. Subject to Transactions & Code Sets (TCS) Deadline?	F. Date TCS Deadline Extension Request Filed
Agency HIPAA Issues			
Personnel	<input checked="" type="checkbox"/> Covered Entity <i>If Covered Entity:</i> <input type="checkbox"/> Payer <input checked="" type="checkbox"/> Provider <input checked="" type="checkbox"/> Business Associate <input type="checkbox"/> Trading Partner	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	Pending
<p>The Department of Personnel is considered a provider due to the counseling services provided to state employees through the employee assistance program.</p> <p>The department oversees the administration of the health insurance plans that are components of the state employee benefits package. IDOP will elect to receive only summary health and enrollment information from the health plans to reduce the HIPAA compliance requirements.</p> <p>The department, through a 28E agreement with the Iowa Department of Public Safety, participates in the administration of the Peace Officers Retirement Fund. This issue is being reviewed to determine if the department is a covered entity as a payer.</p>			
Public Health	<input checked="" type="checkbox"/> Covered Entity <i>If Covered Entity:</i> <input type="checkbox"/> Payer <input checked="" type="checkbox"/> Provider <input checked="" type="checkbox"/> Business Associate <input type="checkbox"/> Trading Partner	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A
<p>Within the Department of Public Health, the Medical Examiner's Office clearly falls under the definition of a HIPAA-covered provider. The department deals with a number of healthcare providers in carrying out various programs, however, it does not directly provide healthcare services or file or process medical claims (containing protected health information) for payment.</p>			

State Agencies With Divisions or Programs That Are HIPAA Covered Entities			
A. State Agency	D. HIPAA Covered Entity Status (Covered Entity Type, Business Associate, Trading Partner)	E. Subject to Transactions & Code Sets (TCS) Deadline?	F. Date TCS Deadline Extension Request Filed
Agency HIPAA Issues			
Public Safety	<input checked="" type="checkbox"/> Covered Entity <i>If Covered Entity:</i> <input type="checkbox"/> Payer <input type="checkbox"/> Provider <input checked="" type="checkbox"/> Business Associate <input type="checkbox"/> Trading Partner	<input type="checkbox"/> Yes <input type="checkbox"/> No	Pending
<p>The department, through a 28E agreement with the Iowa Department of Personnel, administers of the Peace Officers Retirement Fund. This issue is being reviewed to determine if the department is, in fact, a covered entity as a payer.</p>			
Regents	<input checked="" type="checkbox"/> Covered Entity <i>If Covered Entity:</i> <input type="checkbox"/> Payer <input checked="" type="checkbox"/> Provider <input checked="" type="checkbox"/> Business Associate <input type="checkbox"/> Trading Partner		
<p>Within the Regents system, the University of Iowa Hospitals and Clinics operates a number of facilities and employs physicians, dentists, pharmacists, nurses, and other healthcare professionals that fall under the definition of HIPAA covered providers. Additionally, there are the functions performed by the Board of Regents staff and staff at the Regents Institutions that falls under the category of business associate. A HIPAA compliance program is organized and is underway within the Regents system. Charles Wright, Director of Legal Affairs, Human Resources, and Information Systems for the Board of Regents told me the board receives regular updates on the status of HIPAA compliance.</p> <p>Additionally, the project office has been pursuing the availability of an automated HIPAA assessment and compliance documentation tool (called pathfinder) developed by the University Hospitals in Iowa City. We are working on the various software licensing and development cost issues.</p>			

State Agencies With Divisions or Programs That Are HIPAA Covered Entities			
A. State Agency	D. HIPAA Covered Entity Status (Covered Entity Type, Business Associate, Trading Partner)	E. Subject to Transactions & Code Sets (TCS) Deadline?	F. Date TCS Deadline Extension Request Filed
Agency HIPAA Issues			
Veterans Affairs / Iowa Veterans Home	<input checked="" type="checkbox"/> Covered Entity <i>If Covered Entity:</i> <input type="checkbox"/> Payer <input checked="" type="checkbox"/> Provider <input checked="" type="checkbox"/> Business Associate <input type="checkbox"/> Trading Partner	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	August 16, 2002
<p>The Iowa Veteran's Home in Marshalltown is a HIPAA covered entity as a provider of healthcare services. They have organized a HIPAA compliance program with staff throughout the institution. They have completed a HIPAA gap analysis using the document from the project office and are developing their HIPAA compliance strategy.</p>			

Appendix B. State of Iowa Executive Branch Agencies with Only Business Associate Status

State Agencies with Business Associate Status Only (Not HIPAA-Covered Entities)

- Civil Rights
- College Student Aid
- Commerce-Alcoholic Beverage
- Commerce-Banking
- Commerce-Credit Union
- Commerce-Insurance
- Commerce-Professional License
- Commerce-Utilities
- Cultural Affairs
- Economic Development
- Education
- Elder Affairs
- Ethics and Campaign Disclosure
- General Services
- Governor's Alliance on Substance Abuse
- Governor's Office
- Human Rights
- Inspections and Appeals
- Iowa Communications Network
- Iowa Finance Authority
- Iowa Law Enforcement Academy
- Iowa Public Employees Retirement System
- ITD
- Lottery
- Management
- Natural Resources
- Parole Board
- Public Defense - Emergency Management
- Public Defense - National Guard
- Public Employees Relations Board
- Revenue and Finance
- Transportation
- Workforce Development

A **Business Associate** is a person or entity who performs a function or assists a Covered Entity with a function or activity involving the use or disclosure of Protected Health Information (PHI). Examples of functions include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, proactive management, and re-pricing; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. A Covered Entity may be a Business Associate of another Covered Entity.

Proposed HIPAA security regulations require chain of trust agreements between business associates that electronically exchange data. Business associates covered by such agreements must protect the integrity and confidentiality of data exchanged, thereby maintaining security at each link in the chain.

Final HIPAA privacy regulations require business associate agreements between covered entities and business associates with whom individually identifiable health information is exchanged. Business associates are defined as persons to whom the covered entity discloses protected health information so that the person can perform, or assist with performance of activity on behalf of the covered entity. The definition does not include members of a covered entity's work force. It does include individuals or entities that provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services for the covered entity when the provision of services involves the disclosure of protected health information. The

regulations require that business associate agreements be enacted for disclosure of protected health information except disclosure by health care providers to other providers for referral or consultation.

A typical business associate agreement will require that the associate:

- Not use or further disclose information other than as permitted or required by the agreement.
- Report any use or disclosure of information not provided for by the agreement.
- Use appropriate safeguards to prevent use or disclosure of information other than as provided for by the agreement.
- Ensure that subcontractors or agents to whom protected health information is provided agree to the same restrictions and conditions.

Appendix C. The Family Medical Leave Act (FMLA) and Medical Privacy Issues for the State of Iowa as an Employer

Issues of medical privacy and laws relating to the release of confidential information come into play under the Family and Medical Leave Act (FMLA) because the leave law allows employers to request medical certification of the existence of serious health conditions in order to approve absences protected by the statute. In addition, an employer may require a second medical opinion of an employee's medical certification from its own approved provider. In some cases — where the second opinion conflicts with that of the first health care provider — a third opinion can be obtained, which is binding on the parties. Employers also may require that an employee take a fitness-for-duty exam when the employee returns from FMLA leave. These and other questions relating to access to health information raise potential concerns under the rules issued for the Health Insurance Portability and Accountability Act (HIPAA).

The U.S. Department of Labor (DOL) has issued regulations and a model certification form for implementing the FMLA's medical certification requirement. The employer may be limited in the information it may request from the health care provider to what is relevant to the employee's current serious health condition. This may include the following items:

- the medical facts that support the determination that the condition fulfills the FMLA's criteria of a serious medical condition;
- the date the medical condition began and the expected duration of the condition;
- whether leave will be intermittent or on a reduced leave schedule;
- the duration of the leave;
- if the serious medical condition is pregnancy or a chronic condition, whether the patient is presently incapacitated and the duration and frequency of episodes of incapacity; and
- if additional treatments are required, an estimate of the probable number of such treatments.

Consequently, the FMLA does not provide the employer with broad discretion to seek the release of information from the employee's health care provider. Under the statute, an employer may not acquire the employee's medical records or a summary medical report that contains any information beyond that which is set out in the DOL's sample certification form ([Form WH-380](#)). Nor may the employer seek a broad listing of the dates on which the employee was seen by the health care provider, or a description of the nature of the treatment provided (in most circumstances) or allow the disclosure of a diagnosis.

If the employer questions the original certification submitted by the employee, it is permitted to contact the health care provider. However, this query generally is limited to those circumstances in which the employee consents to such contacts. (Exceptions exist if the employee is on a workers' compensation leave in a jurisdiction that allows an employer to directly contact health care providers for workers' compensation-covered absences.) In the typical FMLA case, if consent is provided, the contact must be made by a health care provider acting on the employer's behalf (rather than a supervisor or human resources department staff member initiating such calls). By

regulation, such contacts must be limited to clarifying and confirming the authenticity of the submitted certification.

The FMLA statute does not contain any privacy protections, but DOL regulations require employers to maintain as confidential all "medical certifications, re-certifications or medical histories of employees or employees' families." These records must be maintained in separate files from the usual personnel file and, if the Americans With Disabilities Act (ADA) also applies, maintained according to the ADA's privacy requirements. Employers may disclose this information under the following circumstances:

- Supervisors and managers may be informed about necessary restrictions on the work or duties of an employee and any necessary accommodations;
- First aid and safety personnel may be informed when appropriate if the employee's physical or medical condition might require emergency treatment; and
- Government officials investigating compliance with FMLA or other pertinent law must be provided relevant information upon request.

Like the ADA, the FMLA applies to the employer. The statute does not regulate group health plans directly, although it places requirements on the plans to continue health insurance coverage when an employee is on FMLA leave. Thus, HIPAA and FMLA requirements may overlap regarding group health plans.

Like the ADA, the FMLA allows employers to obtain medical information about their employees for medical certifications and fitness-for-duty exams. There are no specific requirements for the employer to obtain consent or authorization for these disclosures. HIPAA alters this provision by requiring the employer to obtain written authorization from its employees to obtain medical information for this purpose.

There is no specific guidance in the privacy rules adopted under HIPAA on whether a group health plan can disclose medical information to an employer so that the employer may assess a request for FMLA leave. While HIPAA allows group health plans to disclose protected health information to an employer or plan sponsor that has incorporated HIPAA's requirements in its plan document, these disclosures can be made only for plan administration functions. In addition, to allow such a disclosure, the plan document must state that the information disclosed to the plan sponsor may not be used for employment-related purposes. FMLA leave is generally related to employment, not the administration of a group health plan. Consequently, written authorization from the employee appears to be necessary before such a disclosure may be made.

Appendix D. State of Iowa Enterprise HIPAA Project Office Contacts

Project Administrator..... Tom R. Shepherd (515) 725-0294 tom.shepherd@itd.state.ia.us

HIPAA Legal Counsel Janet Hoffman (515) 281-5478 jhoffma@dhs.state.ia.us

Project Office Webmaster..... Scott Krolak (515) 725-0403 scott.krolak@itd.state.ia.us