Privacy and security policy guidance

This section is intended to provide guidance in crafting new policies and procedures or making revisions to existing documents for your organization regarding the federal and state privacy and security laws and regulations. Our hope is the information provided assists your organization to meet the requirements contained within a Business Associate Agreement ("BAA").

The following is a checklist of the minimum BAA requirements you must comply with. You should have the following in place:

- Privacy and security policies
- Provisions for specific uses and disclosures
- Policy or procedure that describes your allowed uses and disclosures in accordance with the Business Associate Agreement
- Administrative, physical and technical safeguards
- Privacy and security training programs
- Confidentiality and/or Nondisclosure Agreements
- Process for reporting of privacy and/or security breaches
- Return/destruction of information upon termination of the BAA

Privacy and security policies

A written privacy and security policy is a valuable tool for your organization. The policy can assist in demonstrating regulatory compliance for privacy and security laws and regulations, and can also be used as an informational tool to demonstrate to consumers how your organization protects its information. Below is a list of common topics typically found in a privacy and security policy for the health benefits industry:

- Type(s) of information protected by the policy would be confidential information (CI) such as individually- identifiable health information/protected health information ("PHI"), financial information, and non-public personal information.
- Classifications of individuals required to follow the policy.
- The administrative, technical and physical safeguards and processes in place within your organization to protect the privacy of the information. This should include actions as required to be in compliance with federal and state privacy and security laws, such as Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economics and Clinical Health Act (HITECH) which was part of the American Recovery and Reinvestment Act of 2009 (ARRA), Gramm - Leach – Bliley (GLBA), Fair Credit Reporting Act, Telephone Consumer Protection Act and other laws designed to protect information.
- Description of the various individual privacy rights provided under the HIPAA Privacy regulations and the appropriate process to follow in the event an individual requests to invoke one or more of these rights. This includes making information available to the covered entity to fulfill a request from a member.
- Descriptions of the uses and disclosures of information including those that are required, those that are permitted without authorizations and those that require an authorization from the individual.
- Guidelines that should be followed for safeguarding information, including, but not limited to: authentication, minimum necessary, disclosure requirements and de-identification of CI requirements.
- The appropriate process for employees to report any suspected breach or policy violation including the notification of such breaches to the covered entity. Please note that under the final Omnibus Rule, business associates are now directly liable for any breach of CI and are subject to possible fines and penalties as a result of such breach of CI.
- The possible penalties for non-compliance of the company policy.

- Description of required Confidentiality and/or Nondisclosure Agreements or executed documents with employees, third parties, contracted individuals, or contracted organizations performing services that involve the use or disclosure of CI. Please note that under the final Omnibus Rule business associates are now required to execute Business Associate Agreements with all of their downstream subcontractors with whom they share CI.
- Description of the program you have implemented to conduct oversight of your subcontractors to ensure they are in compliance with contractual requirements and with applicable Federal and State privacy regulations.

Provisions for specific uses and disclosures

Most agreements contain provisions for specific uses and disclosures of CI that are allowable per the agreement as well as specific restrictions for the use or disclosure of information. The following are examples of common provisions included within the agreement:

- Typically your organization would be able to use CI for the proper management and administration of the Business Associate, or to carry out the legal responsibilities of the Business Associate
- Your organization may use CI for data aggregation to permit data analysis that relates to health care operations for the covered entity
- Most BAAs restrict organizations from using or disclosing CI to only those that are permitted or required by the agreement or as required by law
- Your organization may use CI to report violations to the appropriate Federal and State authorities consistent with HIPAA Privacy regulations

If you are a Humana business associate, in addition to the items listed above, your organization should not directly or indirectly receive remuneration in exchange for any CI of an individual without Humana's prior written approval and notice from Humana that it has obtained consent from the individual.

Administrative, physical and technical safeguards

The following are examples of common safeguards that can assist with the protection of CI. Organization size and available technology should be considered when determining the appropriate safeguards to implement.

Administrative examples

- Designation of an individual responsible for privacy and security concerns and administration of a privacy and security policy.
- Implementation of a company privacy and security policy.
- Privacy and security training programs required for all employees. Ability to provide evidence that training has occurred and is provided to all associates.
- Documented policy that demonstrates removal of system access of employees upon termination or job change.
- Policy that requires the reporting of potential privacy or security breaches to the appropriate covered entity.
- Procedures to manage the selection, development, implementation, and maintenance of security measures to protect information.
- Documented policy to apply appropriate sanctions to associates who fail to comply with the privacy policy and procedures.

Physical examples

- Access controls established for facility, building and office locations.
- Requirement for all CI to be stored in a secured manner overnight (locked file cabinets, locked desks or locked offices).
- Requirement for all CI to be secured when not in use for an extended amount of time (placing documents in desk drawer or filing cabinets).
- Process for mail to be routed to the addressee without the document being opened. For mail without a specific addressee which contains CI, it should be opened and placed in an envelope or folder to protect the information.
- Documents containing CI that are no longer needed to meet retention requirements or other purposes should be destroyed by shredding or placing them in locked, designated areas for shredding.
- Timely retrieval of documents containing CI from printers, copiers, or facsimile machines.
- Enclose hardcopy documents containing CI in envelopes when transporting within facility or through office mail.
- Information other than the address should not be visible through envelope windows.
- Requirement for all incoming faxes to be picked up and secured in envelope or folder if fax contains CI.
- Mobile devices, such as cell phones, smartphones (such as BlackBerry® devices) or laptops should be stored out of sight in a locked desk or cabinet when not in use for an extended period or overnight.
- Block public observation of workstation screens/display monitors whenever possible by closing software application, turning monitors off or away from open viewing areas and walkways, or using filter screens that limit monitor viewing.

Technical examples

- Establishment of restrictions or levels of access to limit data to employees that have a "need to know" (minimum necessary requirement).
- Access controls that include the requirement for changes to access based on job reclassification or employee termination.
- Requirement to use a fax cover sheet for all outgoing faxes containing CI. Fax cover sheet would include a privacy disclaimer on required actions if fax is received by unintended party.
- Requirement for a secure routing mechanism for e-mail containing CI (encryption or password protection).
- Requirement for the proper use of the scan to e-mail function on a multifunction device (a device that consolidates the functionality of a printer, copier, scanner and/or fax into one machine). CI should not be sent to external e-mail addresses from a multifunction device.
- Requirement for a proper method of disposing of CI following state and federal retention requirements.
- Policy on secure access requirements or methods for obtaining CI when working outside of business location or facility.
- Policy on prohibiting the use of mobile devices, including laptops, hand-held devices (BlackBerry's®), etc. that do not provide secure transmission for accessing CI.
- Policy on the use of wireless technology to protect CI (Wi-Fi).
- Establishment of appropriate measure for encrypting and handling media (CDs, floppy disks, DVDs) or hardware containing CI, including receipt into and removal from a facility location, transfer within a facility location, media storage, media re-use and disposal.
- Establishment of appropriate measures to prevent, detect, contain and correct privacy and security violations.
- Policy on requiring frequent system password changes with clear expectations related to password protection (non-disclosure).
- Policy requiring password protected screen savers to disable computer when inactive.
- Requirement for system lockdown of computer workstation when associate is away from workstation for any period of time.
- Requirement for the logging off/shutting down of workstation computers at end of each business day.

Privacy and security training

The following is a list of considerations and suggestions for development of a training or awareness program for your organization. This is intended as a basic guideline on developing your privacy training program and the contents of your program.

- Develop or purchase a training or awareness program that complements the size of your organization.
- Determine method and format to provide training to new employees with consideration for employee locations, availability of technical equipment, applicable software, and language requirements.
- Identify the frequency of your training program.
- Determine the appropriate audience of your training.
- Determine the applicable federal and state regulations that should be incorporated into your training program such as HIPAA, HITECH and GLBA.
- Develop a method to track and record training of employees.
- Determine if an assessment or evaluation is appropriate for your training program.
- Review your company's privacy and security policy to determine contents for your training program. Recommend the following elements be included:
  - — Commitment of your organization on safeguarding and respect for the privacy of information.
  - — Introduction to common terms such as protected health information, personal information, non-public personal information, breach, Business Associate, use, disclosure and covered entity.
  - — Introduction to privacy and security related concepts including, but not limited to, individual privacy rights, minimum necessary standard and Notice of Privacy Practices.
  - — Explanation of procedures to be followed by any contractors or subcontractors using and/or disclosing CI on behalf of your organization.
  - — Procedure for reporting a suspected privacy or security policy violation.
  - — Procedure for appropriate handling of consumer privacy complaints.
  - — Explanation of potential sanctions if procedures and policy are not followed.

Confidentiality/Nondisclosure agreement

As required by most BAAs, your organization shall maintain written confidentiality/nondisclosure agreements with contractors including subcontractors and independent contractors to whom you provide the covered entity's CI. This agreement should be consistent with the terms, restrictions and conditions established in the BAA. Please note that under the final Omnibus Rule business associates are now required to execute Business Associate Agreements with all of their subcontractors with whom they share CI.

In addition, if you are a Humana business associate, your organization should not provide Humana's CI to any contractor including subcontractor and independent contractor outside of the United States of America without Humana's prior written approval.

Reporting a privacy/security breach procedure

As stated previously, your organization should have a process in place for employees to identify and report any violation or potential violation of privacy and/or security. A business associate of a covered entity should notify the covered entity following the discovery of such incident and within the agreed upon timeframes as stated in the BAA. The discovery date is defined within HITECH as the first day on which the incident was known to the company or should reasonably have been known to the company.

All Humana business associates should notify Humana's Privacy Office of any incidents involving Humana member information without unreasonable delay and in no case later than five (5) business days. This notification can be submitted to Humana by completing the Notification of Breach Report form to briefly describe the incident and any steps taken or to be taken to rectify the situation. In addition, the notification should include a description of any investigatory steps taken, list of individuals impacted by the incident, the type of information involved in the incident, the date of the potential incident, and the date of discovery. Breach notifications must be reported to Humana by one of the following methods:

By mail: Humana Inc.
Privacy Office 003/10911
101 E. Main Street
Louisville, KY 40202

By phone: 502-580-3700

By email: privacyoffice@humana.com

Based on the seriousness of the incident, your organization should determine if a telephone call should be made to Humana's Privacy Office prior to the completion of the Notification of Breach Report.

Humana will be responsible for determining whether notification is required to the impacted individuals, media outlets, law enforcement agencies, consumer reporting agencies and any applicable federal or state agencies including the Secretary of Health and Human Services. In addition, Humana will determine the contents of such notice and whether any type of remediation and the extent of any such remediation that may be offered to the impacted individuals.

Humana's Privacy Office will review the information provided and return the document with either signed approval as presented or with additional actions to be taken in order to meet approval by Humana. If additional actions are required, your organization should review the report, provide any additional information including implementation dates and return the document to Humana's Privacy Office. Follow-up monitoring of the action plans included in the report will be performed by Humana's Privacy Office and/or Humana's Delegation Compliance department.

Return/Destruction of information procedure

When the arrangement between your organization and Humana ends, your organization is obligated to return or destroy all Humana member and proprietary information received from Humana and all Humana member and proprietary information created or received on behalf of Humana that your organization still maintains in any form. In addition, your organization should not retain any copies of the information.

If the return or destruction of this information is not feasible, your organization should continue to extend the protections of the BAA and limit further use of such information to those purposes that make the return or destruction of such information infeasible.

Humana requires a written certification of the actions taken by your organization as it pertains to Humana member and proprietary information (return, destruction or protections continued).

Survey requirements

If you are a business associate of Humana, you may be asked to complete a security and privacy survey and/or attestation designed to assist Humana in understanding and documenting your organization's compliance with the requirements of the BAA.

Contact information

You can reach Humana's Privacy Office by email or mail.

Email address
privacyoffice@humana.com

Mailing address
Humana Inc.
Privacy Office 003/10911
101 E. Main Street
Louisville, KY 40202

You can reach Humana's Enterprise Information Security office by email or mail.

Email address
eis@humana.com

Mailing address
Chief Information and Security Officer
321 West Main Street
24th Floor
Louisville, KY 40202

GCA07JBHH 0114