Managing Relationships with Business Associates and Other Third Parties

Kate Borten, CISSP, CISM
The Marblehead Group

Agenda

- ⌘ The life cycle perspective for managing 3rd party relationships
- A. Establishing the relationship
- B. Ongoing management of the relationship
- C. Termination of the relationship

Life Cycle Management

- Business Associates (BAs) and other third parties with access to your Protected Health Information (PHI) [or any other confidential information] must be managed. Your organization's reputation is at risk and you may be legally liable.
- Be sure to manage the relationship start to finish... through the full "life cycle."

Life Cycle Management

Three major stages:

A. Establish the relationship formally
B. Manage and monitor the relationship
C. At termination of relationship, tie up ends

Establish the Relationship

Establish the Relationship

- Start with internal process for identifying all new BAs/3rd parties. Reinforce requirements with managers. Review spreadsheet periodically.
- Good working relationship is not enough. Get all expectations in writing – contract plus additional information – so organizations are on the same page.

Contracts

- Using contract templates (legal review), get contract signed (by *authorized* party) before any access is granted.
- BA contracts must contain language required by HIPAA privacy and security rules.
- Consider similar requirements for other 3rd parties with access to confidential assets.

Contracts

- Contract language should apply to all forms of PHI, not just electronic.
  - Remember the privacy rule's scope and security requirements.
  - Just good practice.

Contract Points – Agents

- Be aware of BA/3rd party's relationships with its agents and sub-contractors. Be sure all relevant HIPAA conditions and restrictions are passed along.
- Consider requiring notice when subcontracting, especially if offshore.

Contract Points – Monitoring and Audits

- Set expectations for monitoring/oversight with the BA/3rd party.
- Consider what level of audit or review may be performed during the contract period.
- Consider requiring BA/3rd party to undergo 3rd party compliance audit (e.g., annually).

Additional Documents – Contact Info

- Require exchange of contact info:
  - Privacy and security officials (and backups?)
  - Include 24x7 contact info such as cell phone
- Require notice of changes in contact info (prior to or at time of change).

Additional Documents – Incident Response

- Specify incident reporting time(s).
- Consider providing guidelines for different incident levels and high-level response actions.
- Ensure that BA/3rd party passes requirements through to sub-contractors also.

Additional Documents – User Access

- If BA/3rd party will need access to your network and systems, require BA to agree to follow your user access policies and procedures including:
  - For obtaining access
  - Access and authentication standards
  - For termination of user access

Manage and Monitor the Relationship

Granting BA/3rd party User Access

- Follow documented authorization procedures (recommendation: require *your* manager be “sponsor”).
- Ensure access privileges set at minimum necessary level required for job.
- Enforce unique IDs and acceptable authentication (recommend 2-factor for remote access).

Controlling BA/3rd Party User Access

- Turn off access unless/until needed, if possible (e.g., for vendor support or BA who only needs access once/month).
- Set all third party user accounts with future expiration date so not open-ended.
- Log 3rd party user activity, and review logs.

Terminating BA/3rd Party User Access

- Enforce BA/3rd party workforce termination procedure that includes notifying “sponsor” and specifies conditions and timing --
  - Prior to termination when anticipated
  - Immediately upon unanticipated termination or if reason for concern
- Be sure every access point is reviewed and all IDs for this user are deactivated.

Monitoring/Auditing 3rd Parties

- Consider reviewing (with advance notice) BA/3rd party privacy & security practices such as:
  - Policies
  - Workforce training procedure and materials
  - User access reports
  - Incident response plan

Monitoring/Auditing 3rd Parties

- If going to review, develop written plans
  - Frequency of review
  - Performed by whom
  - How to evaluate (Compare 3rd party policies and other documents to what?)
  - Consequences?

Terminate the Relationship

Terminating a BA/3rd Party Relationship

- Be prepared. Develop internal guidelines for managing termination.
  - For normal business termination and hostile
  - Plan for how to identify all of this 3rd party's users with access (local and remote). Ensure all accounts are deactivated, access tokens returned, etc.

Terminating a BA/3rd Party Relationship

- Develop guidelines for managing termination.
  - Will PHI and other confidential data be returned or destroyed? Require signoff from 3rd party ("Everything has been destroyed/returned...") and any exceptions.
  - Under what conditions will 3rd party be permitted to keep such data? Get written assurance that data will no longer be used except as described in contract, and that it will continue to be protected indefinitely.

In conclusion ---

- **Be diligent**…. There is heightened risk associated with 3rd parties since they aren't under your direct control and scrutiny.
- And HIPAA makes it the Covered Entity's responsibility. CEs will be held accountable if they should/could have known about a BA violation/breach and done something to prevent it.

Questions?

Kate Borten, CISSP, CISM
President, The Marblehead Group, Inc.
1 Martin Terrace
Marblehead, MA 01945
Tel: 781-639-0532
kborten@marbleheadgroup.com
Web: marbleheadgroup.com