RISK NOTE

Contracts – DSAs for Granting Access to PHI to Third Parties

OVERVIEW OF ISSUE

There has been an increase in the sharing of personal health information (PHI) with parties outside of organizations and an increased potential for privacy breaches arising from that sharing. Examples including PHI being shared with third party contractors and access being granted to employees of other entities (such as physician private practices). It is important that organizations understand how to effectively manage these relationships and ensure they are in compliance with applicable legislation, regulations and privacy protection obligations. Once the decision has been made to grant a third party access to an organization's PHI, organizations should enter into a robust data sharing agreement (DSA) to mitigate the risk of a privacy breach and decrease legal risk if a breach or other issue arises from the third party's access.

KEY POINTS

- HIROC recommends that subscribers have their corporate legal counsel and privacy officer review all agreements.

Refer to related Risk Notes for further details:

- Contracts - Data Sharing Agreements Risk Note

THINGS TO CONSIDER

Managing Liability

- Increasingly, data sharing is becoming an important and essential aspect of the health care business.
- If an organization deems that there is merit to sharing PHI data or access with a third party organization, the organization should first ensure that they are allowed to do so in accordance with the application governing legislation and regulations.
- Prior to granting access to data that includes PHI, organizations should enter into a robust agreement that sets out the terms and conditions of the data sharing relationship.
- In addition to the common clauses contained within a data sharing agreement the following provisions are recommended:
  - Proof of Mandatory Insurance
  - Hold harmless and Indemnity Clause
  - Prohibition on sharing user IDs and Passwords
  - Education
  - Verification and ongoing validation of Users
  - Termination of Access
  - Notification Rights
  - Breach Obligations
  - Auditing Capabilities

Proof of mandatory insurance

- Ensure that cyber coverage is included for all of the third party's authorized agents who are granted access to the organization's PHI.

Hold harmless and Indemnity Clause

- Organizations should ensure that the agreement contains a hold harmless and indemnity clause with respect to civil or tribunal claims for compensation arising a privacy breach caused by the third party or their agents.

Prohibition on sharing user IDs and passwords

- Each individual users should be granted a unique user IDs and password and advised that sharing this information, even amongst other colleagues, is prohibited.
- Organizations should be able to audit all PHI use or disclosure by all third party users at all times.

RISK
NOTE

HIROC

Contracts – DSAs for Granting Access to PHI to Third Parties

Education

- Ensure anyone who is granted access is educated in the proper use, protection and disclosure of PHI in accordance with your organizations policies and procedures and applicable legislation.
- Organizations can require a third party to provide education to its agents as a condition of access.

Verification and ongoing validation of users

- Only grant access to those employees whom partner organizations has "signed off" as having met the terms of the agreement.
- Consider having each unique user sign a document confirming that they understanding the terms and conditions of access in accordance with the DSA.
- Partner organization should be required to re-confirm the accuracy of authorized users on yearly regular (eg. yearly) basis and to advise promptly of any authorized users who depart the partner organization or for whom access should otherwise be terminated.
- Organizations should have a complete and up-to-date list of all third party agents at all times.

Termination of Access

- The organization granting access to data should have the ability to terminate access without notice if an individual or organization breaches the terms of the agreement.
- The third party should be required to immediately notify the organization of any breach of the terms of the agreement.

Notification Rights

- Outline specific requirements for the third party to provide prompt reporting of suspected or verified privacy breaches to the organization.
- Outline specific rights and obligations with respect to sharing of information obtained during resulting investigations.

Breach Obligations

- Outline specific obligations for third parties in the event the third party's agent breaches the DSA and an investigation must be conducted.
- Third parties should be required to cooperate fully and promptly with all investigations.

Auditing

- The granting organization should be allowed to audit the partner organization to ensure compliance with the agreement.
- The organization should consider their capacity for conducting such audits and a reasonable frequency for doing so.

Other Considerations

- Where a physician is seeking access to a patient's data for use in a private clinic, consider having yearly sign-off on the agreement as part of the credentialing process.

Date last reviewed: December 2018