**HIPAA Certification Questionnaire Assessment of Anticipated Recipient**

10/11/2017

The HIPAA Privacy Rule (45 CFR 164.§514(b)) states that

*“A covered entity may determine that health information is not individually identifiable health information only if: (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis that justify such determination [...]”* [emphasis added]

Therefore, it is necessary to obtain some information about the *Anticipated Recipient* and *other reasonably available information* so as to apply appropriate statistical risk models for the given A*nticipated Recipient.* The risk of disclosure can change depending on the level of protection the Anticipated Recipient is able to provide, the anticipated use and further disclosure of the data, and the availability of other data resources the Anticipated Recipient may have access to.

We cover the relevant points about the Anticipated Recipient in Section 1 and about *other sources of information* in Section 2.

**1. Anticipated Recipient**

The Anticipated Recipient must provide complete copies of its Privacy & Security policies. ChangeHealthcare requires submission of physical or electronic (via email) copies. Mere visual review of the required materials is not sufficient for this purpose. Required documents should cover at a minimum the areas listed below

(a) HIPAA Privacy Policies - Prognos Policy : Breach , Prognos Policy : Information Classification, Prognos SOP\_ Safeguarding De-Identified Data

(b) HIPAA Security Policies - Prognos Policy - Security Awareness and Roles

(c) Incident reporting and response policies and procedures - Refer Prognos Policy : Incidence Response, Refer Prognos SoP: Cyber Security & Privacy Incident Management Program

(d) Risk assessment/risk management protocol - Refer Prognos Policy: Risk Management

(e) Management (requirements regarding Data use policies, Data protection policies) of the Anticipated Recipient’s vendors or customers or other third parties (only to the extent such entities may gain access to ChangeHealthcare data, or systems storing ChangeHealthcare data) - Refer Prognos SOP\_ Safeguarding De-Identified Data,

(f) EmployeeTraining requirements - Refer Prognos SOP\_ Training Procedure,

(g) Data Access: Password management, account access protections, use of smart cards, dongles, two-factor authentication etc. - Refer Prognos SoP : Passphrase Management (h) Encryption requirements (data at rest, mobile/portable devices, data transfer) - Prognos SoP : Encryption and Key Management

(i) Physical facility security - Refer Prognos Policy - Facility Access

(j) Disaster recovery policy - Refer Prognos Policy - Disaster Recovery  
(k) Workstation and server security - Refer Prognos Policy - System Access

(l) Remote data access (e.g., via VPN, cloud services) and use of portable devices - Our policies on remote access apply only to PHI. Please see Prognos Policy: Acceptable Use  
 (m) Employee Privacy/HIPAA training practices - Refer Prognos SoP - Training Guidelines (n) Data backup management - NA we do not back up data and rely on S3 redundancy

This documentation is required and serves as the basis for the assessment of the specific Anticipated Recipient of the data which is required under HIPAA for expert determination of de-identification. A range of technologies and practices are available to address these points, and not every available technology or practice is appropriate or required in every situation. The above list is only intended as a guide to the topics that will be looked at, and it is intended to build an as comprehensive as possible description of the data environment in which the Anticipated Recipient will hold ChangeHealthcare data.

If the Anticipated Recipient intends to use cloud services to store ChangeHealthcare information (or otherwise store ChangeHealthcare Data on servers not physically owned and managed by the Anticipated Recipient), please provide the following additional information:

(a) What Cloud Service Provider will you be using to store the ChangeHealthcare Data? AWS

(b) What data protection assurance does the cloud provider make? Specifically -

1. Is there an expectation that data will be accessed by the Cloud provider’s staff as part of usual maintenance? No, the data will not be accessed by any Cloud Provider their sole purpose is hosting. AWS have entered into contracts, including BAAs with Prognos
2. Does the Cloud Provider offer encrypted storage? Yes S3 Server Side Encryption using AES 128 bit with 256 bit encryption Key
3. If so, doestheCloudProvideroffer,and does the Anticipated Recipient intend to use, end-to-end encryption?

We encrypt all data in transit and at rest:

- SFTP over ssh is encrypted by design

- We use AWS S3 encryption for all S3 buckets.

- We encrypt all mounted drives

1. If so, does theCloud Provider required to retain access to the encryption keys? NO, At no time does cloud provider have access or ability to obtain keys to decrypt at rest or in transit.
2. Which of those encryption services, if any, do you intend to use?   
   - SFTP over ssh is encrypted by design

- We use AWS S3 encryption for all S3 buckets

- We encrypt all mounted drives and EBS volumes

(c) Please provide a privacy policy that describes the data security measures the Cloud Provider offers. - See attached document available from AWS

* (d) Where there are options, please identify which measures you intend to select and which ones you do not opt for.
* (e) What access controls to the cloud are in place? Examples include:  
  1. Password Access - Yes
  2. Restricted IP addresses - Yes
  3. Multi-factor authentication (Please define the required authentication controls,  
        
     e.g., dongles, smart cards, mobile phone access codes, hardware tokens, etc.) - 14 Character password - (Something you Know)

Soft Token - Google Authenticator - (Something you have)

* 1. Device IDs limiting access to authorized equipment - NA, we do not manage any network equipment
* (f) Control over data location:Does the Cloud Provider allow you to restrict physical storage of data exclusively on servers in the United States, and if so did you opt for such a limitation? Yes
* (g) Does the Cloud Provider offer limiting access to IP addresses within the United States? Are there any measures beyond those listed in (e) that would aim to prevent unauthorized access via proxy servers, Tor exit nodes, or bots? Please provide any information available (it is understood that some data protection mechanisms may be in place that are not public knowledge). Yes

**2. Access to other sources of information**

The intent of the following questions is to obtain confirmation that Anticipated Recipient employees who use ChangeHealthcare data do not also use PHI or PII; and that the HIPAA standard of de-identification is not compromised by the presence of other sources of information, or the combination of ChangeHealthcare data with such other data assets. This is to provide assurance that workforce members cannot inadvertently or intentionally re-identify the ChangeHealthcare data.

* (a) Does Anticipated Recipient have access to *Protected Health Information* (PHI), and if so, is all such access governed by appropriate Business Associate Agreements (or does the Anticipated Recipient hold such PHI in a role as HIPAA Covered Entity)? Where necessary for the expert determination, ChangeHealthcare may request details about the Anticipated Recipient's use of PHI, including a list of the sources of PHI Anticipated Recipient has access to. No. Anticipated recipients will only have access to the de-identified data which is de-identified by software and certified as de-identified under the expert determination method.   
  (b) Does Anticipated Recipient have access to any *Personally Identifiable Information* (PII) which is not PHI (as covered in (a))? For example, through ownership of such information, by means of licensing or data use/sharing agreements, or as part of any other business activity Anticipated Recipient is engaged in? Examples include, but are not limited to, PII from consumer databases, subscriber lists, PII obtained from Anticipated Recipient's own clients and customers, and any other PII not explicitly excluded below. This question does not apply to information that is legitimately in the public domain, such as public telephone directories, real property registries, drivers license files, voter registries, etc. It also excludes the Anticipated Recipient's Human Resource (HR) data about its own workforce, *provided* such HR information is properly separated from ChangeHealthcare data on servers that are not accessible to any employee with access to ChangeHealthcare data. No. Anticipated recipients will only have access to the de-identified data which is de-identified by software and certified as de-identified under the expert determination method.

(c) Does Anticipated Recipient have access to any *individual health information* (irrespective of whether such information is identified or not, or whether it originates from a Covered Entity or non-Covered Entity). Only list information not yet declared under (a) or (b) above. Examples of sources of individual health information include, but are not limited to, patient assistance programs, health portals, some consumer databases, health related surveys, health-related sales and marketing data, or other data about the health, medical treatment, or provision of medical services to individual patients. We expect that Anticipated Recipients will have access to de-identified claims and Rx data from ChangeHealthcare. Anticipated Recipients currently have access to de-identified lab and claims data from existing partners.

(d) If Anticipated Recipient has de-identified health information derived from PHI (excluding the de- identified data received from ChangeHealthcare), is there a valid statistical HIPAA certification or determination of Safe Harbor conformance for such data? Yes - HIPAA determination

* (e) If Anticipated Recipient has access to person-level information falling into one of the categories (a) – (d) (where applicable, subject to appropriate HIPAA certification or conformance to appropriate de- identification standards such as HIPAA Safe Harbor, as covered in (d)), can you confirm that employees using the ChangeHealthcare data will not have access to any *identified* person-level data (whether from Covered Entities or non-Covered Entities)? Please specify the access protections. Yes. Access to PHI is limited to a small team and is different from the individuals who have access to de-identified data. Technical and administrative safeguards prohibit users from accessing both PHI and de-identified data.
* (f) Ifemployeeshaveaccessto*de-identified*person-leveldatafromothersources(examples include de- identified claims or remit data from sources other than ChangeHealthcare, as well as other de- identified data from other sources, even if non-health related), can you confirm that you have provided, or will provide, appropriate disclosure risk assessments for the ChangeHealthcare data, considering the availability of such other sources of information? (ChangeHealthcare can only provide a disclosure risk analysis for its own data as a standalone data set and not for the combination of its own data with other sources of information).Yes

(g) ChangeHealthcare provides data that is certified to be de-identified as a standalone data set, and any mingling or combination of ChangeHealthcare data with other data sources, even where such sources are de-identified, can change the risk of disclosure. If it is intended to merge or combine ChangeHealthcare Data with third party assets (at a patient or record level), does the Anticipated Recipient have, or will the Anticipated Recipient provide, statistical risk assessments to demonstrate that the combined data remains not personally identifiable pursuant to the HIPAA Privacy Rule? (Note: It is common industry practice to process de-identified data through records linkage tools that will generate anonymous patient lining keys. While the data is statistically de- identified, such records linkage tools operate effectively as “backdoors”, and hence their use is subject to restrictions, and the data can only be certified to be de-identified if such records linkage tools are protected by third party escrow agents, and their use to link and merge data remains subject to HIPAA certification). Yes. Our determination includes multiple data dictionaries, including those fields that will be provided by ChangeHealthcare. Additionally, we contractually prohibit additional linking without a third party HIPAA determination.

Please add any additional topics you feel are relevant to the HIPAA assessment. Thank you very much!