The Joint Commission

Responsible Use of Health Data™ Certification

One Reviewer for One Day Agenda (Virtual)

Time	Activity & Topics	Suggested Organization Participants
8:00 - 8:15 a.m.	**Opening Conference** • Introductions • Brief review of agenda	Data Use leader Organization's certification contact Others at organization's discretion
8:15 - 8:45 a.m.	**Orientation to Responsible Use Initiatives** Topics to be covered include an overview of: • Responsible Use leadership oversite structure • Organization's goals to protect data. • Process to evaluate Responsible Use of Healthcare Data initiatives. Q & A discussion	
8:45 - 9:15 a.m.	**Reviewer Planning Session** Please have the following information available for the Reviewer Planning Session: See *Responsible Use of Healthcare Data – Information Request*	Organization representative(s) who can facilitate secondary data use discussion.
9:15 -12:30 p.m.	**Policy & Process Discussion** Topics to be covered include: **De-Identification Process** • Verify Policies & Procedures for data de-identification. • Verify the HIPAA method utilized for de-identification. • Verify the evaluation method the organization utilizes for each data set and intended use case to identify and implement appropriate HIPAA method? • Identify staff who are involved in the de-identification of data? Verify how the organization determines that the staff are qualified?	Organization team members and other staff who have been involved in and can speak to the secondary use of data process.

Disclaimer: Recording or transcribing this review is strictly prohibited, including the recording and transcribing that can occur with video conference applications. Discovery of any recording activities will result in the immediate cessation of the review and denial of certification.

Time	Activity & Topics	Suggested Organization Participants
	Data Controls • Verify the security infrastructure. • Verify the recognized security standards or best practices the organization utilizes? • Verify the security infrastructure monitoring process. • Verify the policies & procedures the organization utilizes to address security breaches of de-identified data. • Verify the process for receiving evidence of a security certification or independent audit from recipients of data prior to disclosure. • Verify the process to ensure prior to being released, the recipients of the data have policies and procedures in place to monitor compliance with security standards, conduct risk assessments and mitigation and receive and act on notification of security incidents. **Limitations on Use** • Verify the Data Use Agreement (DUA). Ensure the agreement: o Prohibits reidentification of data. o Prohibits linking of data sets without prior written permission of the organization. o Protects the data using reasonable, industry best practices and safeguards. o Describes in detail appropriate and permissible use cases. o Prohibits the sale of deidentified data. o Prohibits sharing with third parties, either wholesale or in derivative works, without prior written permission of the organization	

Disclaimer: Recording or transcribing this review is strictly prohibited, including the recording and transcribing that can occur with video conference applications. Discovery of any recording activities will result in the immediate cessation of the review and denial of certification.

Time	Activity & Topics	Suggested Organization Participants
	• Verify the policy on how DUA terms and conditions apply to any third parties with whom the data recipient allows access to the data. • Verify the process for each data set, the organization maintains oversight of the data either by strict prohibition of redistribution or by allowing redistribution only with prior written permission. • Verify the process for each data set, the organization maintains oversight over linking of data, including an assessment regarding whether such linking increases the likelihood of reidentification. • Verify the organization develops and implements written policies and procedures on how to determine when a data set is sufficiently modified to no longer be considered for redistribution. • Verify that when two or more data sets are linked, the organization reevaluates the risk for reidentification using the appropriate HIPAA method. **Algorithm Validation** • Verify the organization has an initial and recurring process to validate and test algorithms if developed internally by an analytics group, research center, or data science function, and a re-curing co-development process in place to jointly validate the algorithm with the third-party recipient. • Verify the organization implements a process to specify and document use cases and algorithm accuracy thresholds for contextualization into the clinical workflow. • Verify the organization has a process to test internally developed and/or third-party algorithms that at a minimum evaluates algorithms for nondiscrimination against socioeconomic	

Time	Activity & Topics	Suggested Organization Participants
	characteristics in order to address biases in algorithms development. • Verify the organization has a qualified analytics group, research center, or data science function (either internal or contracted) that is responsible for determining whether an algorithm has been tested for the specific population they are serving, accurate contextualization into the clinical workflow, and who may be over- or under-represented in the data sets on which the algorithm is being trained. • Verify the organization educates and trains applicable healthcare staff on the appropriate use of algorithms, including any limitations. **Patient Transparency** • Verify the organization has a written policy and procedures to educate patients using plain patient-centered language on the value of deidentified data to improve healthcare, the potential uses of deidentified data, the process by which patients will be notified of misused data, and responsible healthcare data use the ability of patients to opt-out of data sharing. • Verify the organization has developed and implemented policies and procedures to address patient concerns and/or questions regarding de-identified data which is made available to the public. • Verify the organization has developed and implemented a written policy and procedures for notification in the event of a breach of de-identified data. • Verify the organization has developed and implemented a policy and procedure by which patients may opt out of their de-identified data being disclosed. • Verify the organization has established a Patient and Family Advisory Council or similar	

Time	Activity & Topics	Suggested Organization Participants
	mechanism which is routinely appraised of the organizations policies and procedures related to de-identified data use and sharing of data. **Oversight Structure** • Verify the organization has designated a leader to provide oversite on the disclosure of de-identified data. Oversite includes: o Managing the policies and procedures. o Performing an assessment of risks/benefits to minimizes conflicts of interest when sharing deidentified data sets. o Establishing a multi-disciplinary approach to data sharing that draws upon clinical, research, and other business stakeholders including informatics, innovation, privacy, compliance, and legal functions. • Verify the organization has a governance board to make decisions about the creation and disclosure of de-identified data sets, including consistent criteria to assess and weigh risks, benefits, patient perspectives, research ethics, equity and fairness related to secondary use of deidentified data. • Verify the data governance board meets regularly with the Patient and Family Advisory Council or similar mechanism, to consider patient input regarding the organizations' policies and procedures related to de-identified data use and sharing and adequacy of patient education efforts. • Verify that the organizations' decision-making processes related to de-identified data include the consideration of equity and fairness.	
12:30-1:00 p.m.	**Reviewer Lunch**	

Disclaimer: Recording or transcribing this review is strictly prohibited, including the recording and transcribing that can occur with video conference applications. Discovery of any recording activities will result in the immediate cessation of the review and denial of certification.

Time	Activity & Topics	Suggested Organization Participants
1:00-1:30 p.m.	**System Tracer – Performance Improvement** Topics to be covered include: • Security Monitoring • Re-evaluation of data sets • Action Plans • Future Initiatives	Data Use leader Administrative and clinical leadership involved in the secondary data use performance improvement plan. Others at organization's discretion
1:30-2:00 p.m.	**Competence Assessment** This session focuses on staff or contracted staff responsible for data security. • Determination of qualifications • If contracted staff, review contract for qualifications • Personnel file review • On-going assessment of competence	Individuals responsible for the organization's human resources process that supports secondary data use. Individuals responsible for assessing staff competency in this area
2:00 – 2:30 p.m.	**Summary Discussion/Report Preparation** This time is reserved for a final discussion prior to the reviewer's report preparation and the exit conference.	Will vary as requested by the review
2:30-3:00 p.m.	**Exit Conference** Reviewer presentation of certification observations and requirements for improvement	Organizational leadership Others at the discretion of the organization

Note: This agenda is a guide and may be modified based on organizational need and reviewer discretion.

Disclaimer: Recording or transcribing this review is strictly prohibited, including the recording and transcribing that can occur with video conference applications. Discovery of any recording activities will result in the immediate cessation of the review and denial of certification.