Third-Party Data Disclosure Risk Management for Healthcare Organizations

Save to myBoK

By April Carlson, MBA, HCISSP, CFE; Daniel Goldman, JD; Burke Milnes, MPA; Kimberly Otte, JD; and Morgan Schacht, JD

Hoping to balance the competing demands to share information while also protecting it, Mayo Clinic has developed a process to review disclosures of data that is risk-based, standardized, and cross-disciplinary.

The challenges facing the American healthcare delivery system are glaringly apparent to everyone—costs are too high, access to healthcare services is too limited, and the quality of medical care is lacking when compared to other developed nations. While lawmakers continue to debate the public policy solutions to this vast problem, Mayo Clinic has explored its own solutions for improving these issues by rethinking the traditional means of delivering medical care and trying to improve care through new, innovative means that utilize the latest technology. Examples include:

- Telemedicine technology to reach patients in underserved areas of the country.
- Predictive algorithms that will indicate which patients are most likely to benefit from individualized care coordination services.
- Analysis of aggregate protected health information (PHI) to determine if a change made to a procedure improved the hospital's infection rates.
- Encouraging patients to report their own medical information—such as blood pressure, blood sugar levels, weight, symptoms, etc.—in a manner that will allow the healthcare provider to remotely monitor the patient's daily condition.
- Use of new technology to accelerate research efforts in developing new life-saving treatments.
- Creation of online patient accounts and health information exchanges to increase accessibility of medical records for patients and their other healthcare providers.

While Mayo Clinic is dedicated to pursuing these solutions and ideas, institutional leadership quickly realized that these more innovative means of providing and managing care pose some significant challenges.

Challenges to Address

Mayo Clinic realized that the institution has an abundance of highly talented medical professionals and administrative staff who specialize in healthcare, but it did not have the internal expertise to develop or replicate the rapidly changing technological innovations that were occurring outside of the hospital walls. This motivated Mayo Clinic to approach external technology companies and other specialists ("third parties") that could provide the technology solutions needed to meet the goals of improving cost, quality, and access. As clinical departments at Mayo Clinic began to rethink their care delivery strategies, the volume of requests to engage external technology solutions increased dramatically and became nearly unmanageable.

In the midst of this increased demand for external technology solutions and services, Mayo Clinic was ramping up its information security efforts in response to the increasing number of significant cyberattacks and breaches occurring in the healthcare industry. The transition from paper medical records to electronic health records was an incredible advancement from a clinical care perspective, but it also made enormous amounts of health information more accessible—and vulnerable—than ever. Hackers are motivated to target patient data because it generally has a higher resale value on the dark web than other types of personal information.[1] A successful hacker can steal the identity of millions of patients or encrypt a hospital's servers to block access to medical records until a ransom is paid.

Managing Competing Objectives

Mayo Clinic was faced with competing objectives: leverage PHI to decrease costs, improve quality, and increase access to care while also enhancing the protection and security of that same data. From an information security perspective, allowing third parties to receive, store, and/or access PHI posed greater risks. Yet, many of the technology initiatives that Mayo Clinic wanted to pursue would have been too costly and inefficient to develop without the assistance of a third party with the necessary technological expertise.

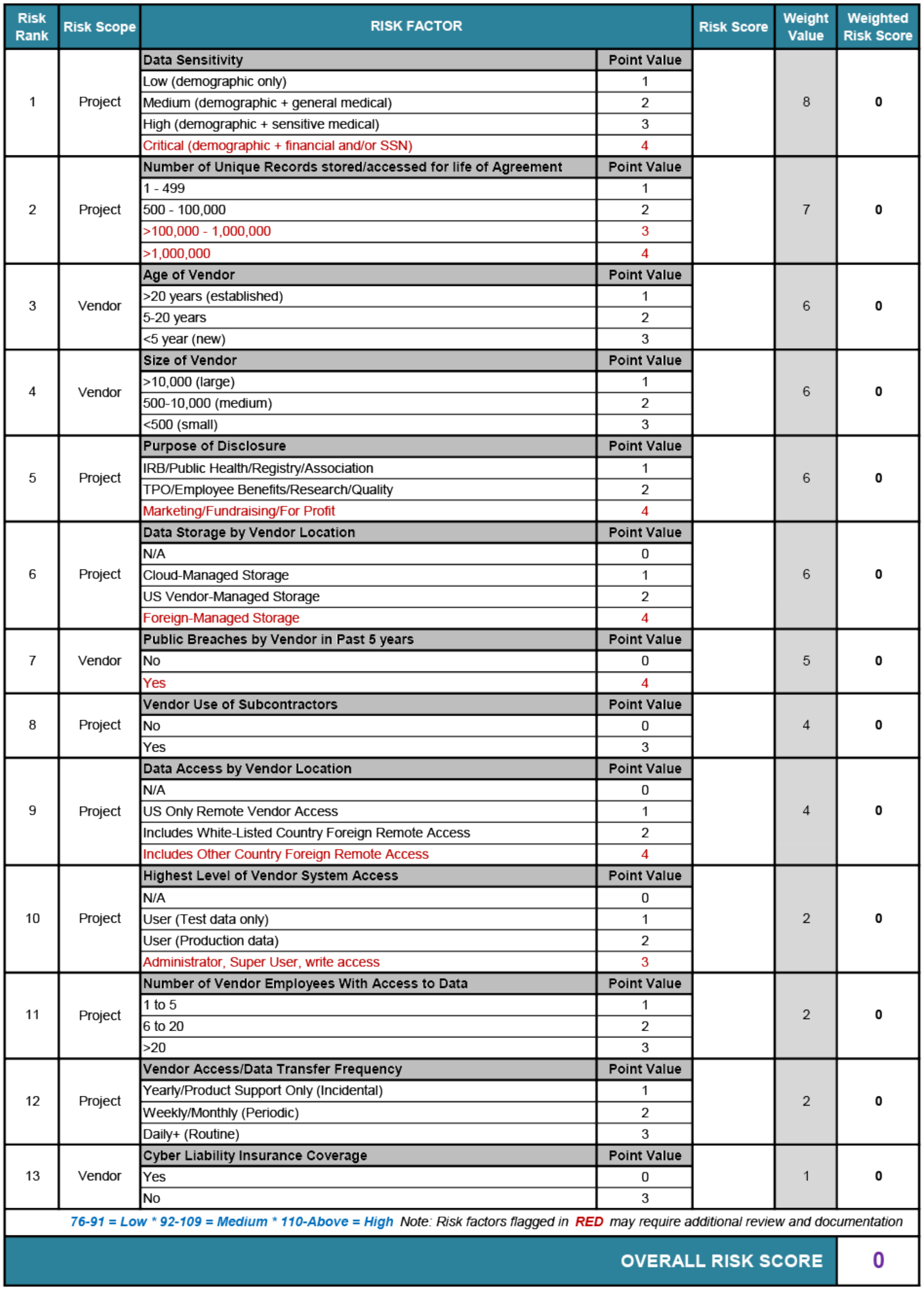
There are many risk-related questions that arise when examining requests to disclose data. For example, what types of information security assurances and safeguards should be required for the third parties who have access to PHI? Should a large, well-established third party receive the same degree of scrutiny as a small start-up company with a cutting-edge technology product to sell? How does a healthcare system manage and coordinate the enormous volume of requests to share PHI with third parties? How should a healthcare system manage subcontractors, offshoring, and non-standard contract terms? How does an institution protect ownership of their data and the intellectual property value it holds when it's de-identified? Will other types of identifiable data held by Mayo Clinic, such as the personally identifiable information (PII) in its role as an employer and academic institution, undergo the same level of review as PHI?

Developing a Risk-Based Framework

Mayo Clinic leadership recognized that large-scale data transfers of sensitive PHI and PII needed sufficient oversight and governance on an ongoing basis and as a result established a Data Disclosure Oversight Committee (DDOC). The organization has a long history of utilizing multi-disciplinary teams in clinical practice areas. Aligning with this tradition, the committee membership is strategically comprised of a multi-disciplinary team of experts bringing their perspective and expertise to the table. The committee includes representation from the clinical practice, privacy, legal, risk, information security, IT, supply chain, and business development departments to help ensure that a broad range of risks are considered during reviews. The cross-disciplinary membership is essential for expertise and to serve as a check and balance for the proponent who often is motivated by a narrower agenda. Internal policies were established requiring DDOC review of external transfers of PHI and PII during both the initiation of new third-party contracts as well as during contract renewal phases.

The committee prioritized deploying a balanced approach to supporting business and practice priorities while helping to carry out sufficient governance and oversight of external data transfers to third parties. They agreed that risks associated with data transfer requests warrant examination, risk mitigation, and, in certain circumstances, formalized risk acceptance. Early in its inception, the committee acknowledged the importance of leveraging a risk-based approach for reviewing data transfer requests and emphasized the importance of leveraging risk-based principles for vendor management. As the review process evolved and matured, DDOC identified common risk categories that consistently surface in data transfer requests. A strategic priority was placed on documenting these common risk categories to develop a corresponding risk scoring framework to consistently calculate risk using a standard set of principles. The risk scoring criteria promotes a more standardized review and consistent measurement of associated risks.

Figure 1: Mayo Clinic Data Disclosure Oversight Committee Risk Scoring Criteria



Risk Rank	Risk Scope	RISK FACTOR		Risk Score	Weight Value	Weighted Risk Score
1	Project	**Data Sensitivity**	**Point Value**		8	**0**
		Low (demographic only)	1			
		Medium (demographic + general medical)	2			
		High (demographic + sensitive medical)	3			
		Critical (demographic + financial and/or SSN)	4			
2	Project	**Number of Unique Records stored/accessed for life of Agreement**	**Point Value**		7	**0**
		1 - 499	1			
		500 - 100,000	2			
		>100,000 - 1,000,000	3			
		>1,000,000	4			
3	Vendor	**Age of Vendor**	**Point Value**		6	**0**
		>20 years (established)	1			
		5-20 years	2			
		<5 year (new)	3			
4	Vendor	**Size of Vendor**	**Point Value**		6	**0**
		>10,000 (large)	1			
		500-10,000 (medium)	2			
		<500 (small)	3			
5	Project	**Purpose of Disclosure**	**Point Value**		6	**0**
		IRB/Public Health/Registry/Association	1			
		TPO/Employee Benefits/Research/Quality	2			
		Marketing/Fundraising/For Profit	4			
6	Project	**Data Storage by Vendor Location**	**Point Value**		6	**0**
		N/A	0			
		Cloud-Managed Storage	1			
		US Vendor-Managed Storage	2			
		Foreign-Managed Storage	4			
7	Vendor	**Public Breaches by Vendor in Past 5 years**	**Point Value**		5	**0**
		No	0			
		Yes	4			
8	Project	**Vendor Use of Subcontractors**	**Point Value**		4	**0**
		No	0			
		Yes	3			
9	Project	**Data Access by Vendor Location**	**Point Value**		4	**0**
		N/A	0			
		US Only Remote Vendor Access	1			
		Includes White-Listed Country Foreign Remote Access	2			
		Includes Other Country Foreign Remote Access	4			
10	Project	**Highest Level of Vendor System Access**	**Point Value**		2	**0**
		N/A	0			
		User (Test data only)	1			
		User (Production data)	2			
		Administrator, Super User, write access	3			
11	Project	**Number of Vendor Employees With Access to Data**	**Point Value**		2	**0**
		1 to 5	1			
		6 to 20	2			
		>20	3			
12	Project	**Vendor Access/Data Transfer Frequency**	**Point Value**		2	**0**
		Yearly/Product Support Only (Incidental)	1			
		Weekly/Monthly (Periodic)	2			
		Daily+ (Routine)	3			
13	Vendor	**Cyber Liability Insurance Coverage**	**Point Value**		1	**0**
		Yes	0			
		No	3			
*76-91 = Low * 92-109 = Medium * 110-Above = High* *Note: Risk factors flagged in* ***RED*** *may require additional review and documentation*						
					OVERALL RISK SCORE	**0**

[View PDF](https://bokold.ahima.org/doc?oid=302750)

Standardized Data Disclosure Risk Scoring Criteria

Figure 1 above illustrates the standard risk scoring criteria developed by the Mayo Clinic's DDOC that is utilized within the Data Disclosure Program. The overall risk scoring equation possesses a combination of vendor-specific and project-specific risk categories. The weight given to each of the risk scoring subcategories was assigned based on committee dialogue, consensus, and documented risk mitigation priorities.

Data Volume and Data Sensitivity

Heavy emphasis is placed on the volume of individually identifiable records to be disclosed as well as the sensitivity level of the data. Data sensitivity risk calculations are rooted in the potential patient, employee, reputational, legal, and financial impact associated with certain types of data being breached. For example, a breach of names and Social Security numbers is scored as higher risk than patient names and demographic medical information such as medical record numbers because of the anticipated patient impact, financial costs, and reputational impact incurred by a data breach with higher sensitivity. Sensitive medical data categories such as substance abuse records, HIV and pregnancy records, or behavioral health records score as higher risk than names and medical record numbers alone.

Vendor-Specific Risk Profiling

Some risk categories focus specifically on the vendor versus the project. For example, one factor in the risk score is how long a vendor has been doing business, as this often correlates with the maturity of its information security program as well as its ability to indemnify for financial damages associated with a large-scale data breach. Following similar logic, the size of the vendor is also calculated in the risk score equation, recognizing that most large companies devote significant resources to build strong information security programs and practices. Additionally, the risk score calculation factors whether a company under review has experienced a significant breach within the past five years. This scoring criteria promotes transparency around past breach occurrences and may serve as a catalyst to obtain additional information as evidence of mitigating controls that have been implemented as a result of the breach.

Data Storage by Vendor Location

Proposed vendor storage type also factors into the risk score calculation. The emergence of vendors that provide cloud storage services was initially considered higher risk. But as the committee began to better understand the stronger information security controls and validated security testing by third-party auditors, it changed the risk profile of reputable cloud storage providers to be lower risk. Additionally, vendor storage clouds that remain in the United States are scored as lower risk than an offshore vendor storage location due to the uncertainty regarding regulatory and vendor controls in place in non-US countries.

Use of Subcontractors

While a vendor may possess a strong information security program, their subcontractors may have less rigorous information security practices and controls. The extent to which a vendor subcontracts out services that involve the storage or processing of data presents additional risk considerations and is therefore factored into the overall data disclosure risk equation. If a vendor discloses that some of the data will be transferred to or accessed by subcontractors as part of the proposed arrangement, this is factored into the overall risk score. The disclosure of data to subcontractors may warrant a more detailed review depending on the overall risk score calculation.

Data Access by Vendor Location and Levels of System Access

The risk scoring criteria also accounts for whether the vendor will hold remote access to Mayo Clinic systems and, if so, from where the remote access will occur. The committee developed guidelines surrounding proposed offshore access and/or storage by location and has documented “white-listed” countries based on information available from corruption and cybersecurity rankings. Countries that are not on the white list require committee review and approval, and they may be approved as a one-off or added to the white list based on the committee’s recommendation. Also factored into the risk equation is the provisioning level of remote access.

The risk scoring criteria also examines what type of data the vendor would have access to remotely. Will a vendor be given access to only test data or does the pending contract propose access to production data? Or, a higher risk, does a particular proposal require the vendor to obtain administrative rights to access internal systems as part of the project?

Number of Employees with Access, Data Transfer Frequency, Cyber Liability Insurance

Risk scoring also takes into account how many third-party employees will have access to the data, how often the transfers will be occurring, and whether the vendor possesses cyber liability insurance coverage.

Operationalizing Standard Data Transfer Requirements

As the data disclosure review process has matured, standard processing guidelines for staff have been created to process requests according to risk calculations. The calculated risk score defines what type of review path a request will take. Moderate risk requests require certain third-party information security evaluations be reviewed before the transfer of data can commence. High-risk requests require a more in-depth examination of information security controls through completion of additional documentation and submission of information security audit reports completed by independent third parties.

The committee has also recognized that contractual assurances are an important part of vendor risk management. Accordingly, the committee requires that vendors execute appropriate agreements including language that not only ensures compliance with regulatory requirements but also industry-standard process and information security controls. Deviations from these institutional requirements must be reviewed and approved by the committee. Expedited approval processes were developed for requests that conform to standard requirements. The operational process is intentionally designed to surface only the highest-risk requests for full committee review, discussion, and approval.

Risk Mitigation through the Review Process

Data disclosure reviews mitigate data privacy and security risks in a number of ways. DDOC staff continually provide guidance to requestors throughout the entire process. Part of the review process centers upon ensuring that the business case to transfer the data is strong and that only the minimum amount of data necessary to meet business or practice needs is transferred to the third party. DDOC staff suggest best practices or other options that make the request lower risk, and thus such requests are more likely to be approved by the committee. As a result, the initial request that is submitted to DDOC often looks significantly different than the request that is ultimately approved.

DDOC advises sending the minimum amount of data elements necessary to meet business objectives and challenges proponents submitting requests to examine what type of data needs to be disclosed. One example involved a proposal to send facial images, behavioral health records, and MRNs to a third party as part of a data sharing arrangement to engage in industry benchmarking. When asked for the business case on why these types of data elements would be required for surgical benchmarking, confirmation was received that these data elements would not be needed by the third party.

DDOC reviews routinely minimize the type of data elements sent to a particular business associate. Other examples of where the committee provides value involve leading effective enforcement of institutional information security standards before data can be sent. Some proposed high-risk data transfers are postponed until the vendor can provide sufficient security assurances and attestations from third-party audit firms. During other reviews, it may be discovered that vendors are unwilling to meet minimum contractual data protection standards and therefore business proponents are advised to explore alternative options with other third parties that are able to agree to institutional data protection contractual provisions. Once a request has been approved, the vendor is added to a “dashboard” through the use of a vended solution. This dashboard enables DDOC to effectively monitor approved vendors for events that may significantly affect the risk profile of an approved vendor such as bankruptcies, data breaches, and/or acquisitions.

Integrating the DDOC Process with a Broader Technology Assurance Process

After the Data Disclosure Program was fully established and operational, colleagues in IT and information security diligently worked to establish a more streamlined and robust review of information technology-related requests. A process was created to help ensure technology- and data-related requests are able to meet technical data protection and IT architectural standards that promote implementing strong information security controls as well as IT system congruence. This process, known as the Security, Privacy, Architecture, and Data (SPAD) assurance process, is intended to be a single entry point to obtain necessary data disclosure, information technology, and information security reviews of a particular request to disclose data. This process helps to ensure sufficient technical expertise is devoted to reviewing a third party’s ability to meet Mayo Clinic data privacy and information security standards. The data disclosure review process was strategically integrated with this broader review process to help promote efficiency and streamlined reviews of data sharing requests.

Developing an effective framework to prudently manage the risks associated with data sharing will be more critical than ever before as healthcare organizations continue to manage divergent priorities—sharing large sets of patient data in ways that fuel innovation while also keeping patient privacy and information security at the forefront.

Note

1. Francis, Ryan. “Healthcare records for sale on Dark Web.” CSO. April 24, 2017. www.csoonline.com/article/3189869/healthcare-records-for-sale-on-dark-web.html.

April Carlson (carlson.april@mayo.edu) is privacy officer/data protection officer, Daniel Goldman is legal counsel, Burke Milnes is Arizona compliance and privacy officer, Kimberly Otte is chief risk officer, and Morgan Schacht is contract manager at Mayo Clinic.

Article citation:
Carlson, April. Daniel Goldman, Burke Milnes, Kimberly Otte, Morgan Schadt. “Third-Party Data Disclosure Risk Management for Healthcare Organizations.” *Journal of AHIMA* 90, no. 6 (June 2019): 18-22.