Government mandates, data sharing agreements and spreadsheets sow confusion amid an avalanche of private data.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>3</td>
</tr>
<tr>
<td>Study Background and Methodology</td>
<td>4</td>
</tr>
<tr>
<td>Demographics</td>
<td>5</td>
</tr>
<tr>
<td>Firmographics</td>
<td>9</td>
</tr>
<tr>
<td>Data Privacy Management Budgets</td>
<td>11</td>
</tr>
<tr>
<td>Projects Impacted by Data Privacy Concerns</td>
<td>15</td>
</tr>
<tr>
<td>Data Sharing Agreements</td>
<td>18</td>
</tr>
<tr>
<td>Technical Data Privacy Maturity</td>
<td>21</td>
</tr>
<tr>
<td>Organizational Data Privacy Maturity</td>
<td>28</td>
</tr>
<tr>
<td>Regulatory Preparedness</td>
<td>35</td>
</tr>
<tr>
<td>Opinions on Federal Privacy Law, and Trust</td>
<td>37</td>
</tr>
<tr>
<td>About Integris Software</td>
<td>40</td>
</tr>
</tbody>
</table>
Executive Summary

Companies are being inundated with data. A single healthcare transaction may get replicated across a hundred data repositories. Healthcare companies are constantly consuming and sharing information to build better patient profiles and improve outcomes. In addition, as healthcare companies consolidate through mergers and acquisitions, they acquire unknown datasets and data transfer agreements with new business partners. In this environment, it’s no wonder that respondents’ data privacy programs scored much lower on technical maturity than on organizational maturity.

Key Findings:

Data privacy management overconfidence: 70% were Very or Extremely Confident in knowing exactly where sensitive data resides yet 50% of them update their inventory of personal data once a year or less; and a mere 17% of respondents are able to access sensitive data across five common data source types.

Data privacy impacts much more than regulatory compliance: Proving compliance with business obligations like data sharing agreements was cited by 67% of respondents. Enforcing internal data handling policies like classification and retention was cited 61% of the time. About a quarter of respondents cited the impact on M&A due diligence (28%) and the delivery of AI / ML projects (22%). About one third saw privacy concerns impacting data lake hygiene (35%).

The proliferation of data sharing agreements: In the wake of the misuse of data sharing agreements like the one between Facebook and Cambridge Analytica, enterprises seem to be more aware of such agreements. But data sharing agreements are nothing new to the healthcare industry. 50% of healthcare industry respondents had 50 or more of these data sharing agreements in place (20% more than the entire set of respondents). However, respondents reported being 61% more confident in their ability to be compliant compared to how they perceived their partners.

Data privacy management budgets reside in IT departments: 52% of data privacy budgets are concentrated in IT departments. Technology leaders are increasingly being tasked with operationalizing their companies’ data privacy management program. Why? At its core, data privacy is a data issue, and privacy is an outcome of a comprehensive data protection strategy.
Study Background and Methodology

This study seeks to understand how mid to large-sized US enterprises manage data privacy within their organizations, as well as their future plans. In February 2019 a web survey was emailed to members of an exclusive community of top business executives and IT decision makers. 258 respondents completed the survey. This version of the study provides a deep dive into healthcare industry cohort which included 46 companies. However, each of the 258 respondents had to meet the following criteria:

- Reside in the USA
- At least “Somewhat Knowledgeable” on how data privacy and data security are managed at their current company
- Mid to senior level professionals and executives
- 500 employees or more (62.4% had over 5,000 employees)
- $25 million or more in annual revenue (69.38% had over $1 billion in annual revenue)
- Functional roles/areas had to be in IT, general management, or risk and compliance

Note: unless otherwise noted, N = 46

What is your personal level of knowledge on how data privacy and data security are managed at your current company?

- Extremely Knowledgeable: 26.09% (It’s part of my primary role)
- Very Knowledgeable: 50.00% (It’s part of my role)
- Somewhat Knowledgeable: 23.91%
Demographics

Respondents had to be, at a minimum, mid-level professionals.

Which one of these is the best fit to your current seniority level?

- 23.91% Senior Professional
- 23.91% Manager, Sr. Manager
- 23.91% Director, Sr. Director
- 6.52% VP, SVP, EVP
- 23.91% C-Level Executives

Demographics: Respondents had to be, at a minimum, mid-level professionals.
Demographics

Respondents came from three key areas of the business:

1. Information Technology/Engineering (67.39%),
2. General Management/Strategy (21.74%) and
3. Legal/Compliance/Risk Management (10.87%).
Demographics

Respondents saw themselves as taking on a range of roles with most having multiple roles as part of their mandate.

Over a third of respondents claimed privacy management fell into their primary role.
Demographics

Within their primary roles, most respondents had either primary/final decision making authority, or were on the decision making committee/had significant influence.

You’ve mentioned that the following are a part of your primary role. Please indicate your personal decision making involvement for each within your current company:
Firmographics

Multiple departments impact decisions related to data privacy. Data privacy management is clearly a multidisciplinary endeavor. Among healthcare industry respondents, data governance was cited the most often (66.67%) as having an impact on decisions related to data privacy vs. 46.9% for all respondents. Perhaps not surprising given the critical role data governance plays in healthcare information management—making sure that health information is accurate, private, and secure.
Firmographics

71.74% of firms had over 1,000 employees.

Approximately how many full-time employees are employed by your company at all sites and locations? If unsure, please provide your best estimate.

- 58.70% 5,000 employees or more
- 28.26% 1,000 to less than 5,000 employees
- 13.04% 250 to less than 1,000 employees
Data Privacy Management Budgets

Companies are dedicating serious resources to data privacy management. 77.50% had budgets dedicated to data privacy management.
Data Privacy Management Budgets

Almost half (47.83%) of healthcare data privacy management budgets in 2018 were between $100K and $500K, which is a much higher concentration than the 32.43% concentration for all respondents.

This variance may be partly due to the fact that the healthcare industry has had to operationalize data privacy much earlier than other industries.
Data Privacy Management Budgets

Over half (51.62%) of data privacy budgets are concentrated in IT departments (InfoSec, data infrastructure, IT operations, and software development). 29.03% of budgets are concentrated in legal, risk, and compliance departments. A mere 3.23% of data privacy budgets are concentrated in the privacy management department. In 6.45% of organizations, it’s not clearly defined.

Healthcare technology leaders are increasingly being tasked with operationalizing their data privacy management program. Why? At its core, data privacy is a data issue, and privacy is an outcome of a comprehensive data protection strategy.

In which department does the majority of data privacy budget reside?
Data Privacy Management Budgets

Unsurprisingly, most healthcare organizations (86.21%) are increasing their data privacy management budgets in 2019. Over a quarter (27.59%) of respondents are increasing their data privacy management budgets by 25% or more.
Projects impacted by Data Privacy

The regulatory environment continues to drive urgency around projects to prove regulatory compliance (76.09%), which includes responding data subject access requests (58.70%), enforcing data retention and classification policies (60.87%), and responding rapidly to breaches (60.87%).

But data privacy impacts much more than regulatory compliance efforts. When done right, data privacy management supports the broader healthcare information management control framework—regulations, policies, and contracts. For example, proving compliance with business obligations like data sharing agreements was cited by 67.39% of respondents.

Which, if any, of your current company’s projects are currently impacted by privacy concerns? Please select all that apply.

- Proving regulatory compliance: 76.09%
- Proving compliance with business obligations like data sharing agreements: 67.39%
- Responding to data subject access requests: 58.70%
- Enforcing data retention and classification policies: 60.87%
- Responding rapidly to breaches: 60.87%
- Staying in compliance when migrating apps to the cloud: 56.52%
- Scanning & tagging data flowing in and out of data lakes: 34.78%
- Accelerating AI / ML projects: 21.74%
- Assessing risk in M&A transactions: 28.26%
- None of the above: 6.52%
- Other (please specify): 2.17%

Which, if any, of your current company’s projects are currently impacted by privacy concerns? Please select all that apply.
Projects impacted by Data Privacy

Data lakes ingest disparate pieces of patient data from a variety of sources. When combined, this data has the potential to reveal customer identities along with highly sensitive personal information. So, it’s no surprise that over a third of respondents (34.78%) cited the impact of privacy for projects that scan and tag data flowing in and out of data lakes.

As data is acquired through the M&A process, data lakes and other datasets can become contaminated with unexpected, inappropriate, or problematic data. Increasingly (28.26%), M&A due diligence includes the inspection of the data being acquired. This allows healthcare organizations to properly evaluate the risk prior to merging large datasets.

Finally, when data is locked down for fear of misuse, data scientists don’t get timely access to the streams and feeds they rely on for their machine learning models.

So, it’s no surprise that AI / ML projects were cited by over one in five respondents (21.74%).
Data Privacy Now Integral to Data Protection

Forward looking healthcare organizations are treating privacy as part of a broader data protection strategy where privacy tells you what’s important and why, and security is the how.

<table>
<thead>
<tr>
<th>Data Protection</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privacy</strong></td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>Discovery &amp; Classification</td>
<td>DSARs</td>
</tr>
<tr>
<td>Regulations</td>
<td>Contracts</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
</tr>
<tr>
<td></td>
<td>Activity Monitoring</td>
</tr>
</tbody>
</table>

What data is important and why

How those policies get enforced

Protected Usable Data
Data Sharing Agreements

50% of respondents had 50 or more data sharing agreements in place. That’s a variance of 20% more than all respondents. This is probably due to the highly intertwined nature of the healthcare industry (EHRs, insurance, etc.).

How many data sharing agreements does your current company have where data is either entering or leaving your organization?

- 50% of respondents had 50 or more data sharing agreements in place. That’s a variance of 20% more than all respondents. This is probably due to the highly intertwined nature of the healthcare industry (EHRs, insurance, etc.).
Data Sharing Agreements

Respondents were much more confident in their own ability to respect data sharing agreements than their partners’ ability to reciprocate in kind (there was a 60.91% increase in Very confident and Extremely confident levels in their own compliance efforts vs their partners).
Data Sharing Agreements

There’s often a disconnect between what has been agreed to on paper by lawyers and what’s happening with the actual data, because the people who negotiate the contract differ from those shipping the data and/or there are no controls in place.

Also, the way contracts are written is not necessarily the way data is represented. The word "location" might appear in a contract, but the data set contains latitude and longitude values. Therefore, businesses must account for how data elements might be combined to fit the legal terms on their data sharing agreements.

How confident are you that your partners are using the data that you provide to them in compliance with your data sharing agreements?

- Extremely confident: 7.14%
- Very Confident: 33.33%
- Somewhat confident: 52.38%
- Not so confident: 7.14%
- Not at all confident: 7.14%
Data Privacy Management
Technical Maturity

Surprisingly, non of the healthcare industry respondents expressed a lack of confidence in their company’s ability to define what is personal information. 32.61% said they were very confident and 34.78% said they were extremely confident.

Are respondents falling victim to overconfidence? Perhaps. Sensitive data has an evolving nature. What’s considered a sensitive category or piece of data today may not be considered sensitive tomorrow, and vice versa.

Understanding derivative personal data is important, yet challenging. For example, notes on patient’s diet can infer religion.

Data flowing in and out of data lakes is also a blind spot for many respondents. Data lakes ingest disparate pieces of customer data from a variety of sources. When combined, this data has the potential to reveal customer identities along with highly sensitive personal information.
87% of the US population can be identified using only their Zip Code, Gender, and Birthdate. *

*Source: https://dataprivacylab.org/projects/identifiability/paper1.pdf
A single healthcare transaction may get replicated across a hundred data repositories. Healthcare companies are constantly consuming and sharing information to build better patient profiles and improve outcomes. In addition, as healthcare companies consolidate through mergers and acquisitions, they acquire unknown datasets and data transfer agreements with new business partners.

In this environment it’s not surprising that over half (52.63%) of respondents said they needed to access 50 or more data sources to get a defensible picture of where their sensitive data resides.
Data Privacy Management
Technical Maturity

Yet 50% of respondents take inventory of personal data less than once a year or in reaction to an audit.
Continuous defensibility to meet compliance requirements boils down to doing two things well:

1. Understanding where sensitive data resides across all data source types.

2. Mapping data back to existing data handling obligations.

Point one was a mixed bag among survey respondents. Traditional data sources like relational databases are included in most (88.37%) data privacy initiatives. Cloud-based applications had good coverage (71.43%), as did unstructured data (66.67%). But data in-motion appears to be the laggard at 50.78%.

Analyzed another way, an alarmingly low 17% of respondents were including all five data types in their company’s data privacy initiatives.

Which, if any, of the follow data types are included in your current company’s data privacy initiatives?
Data Privacy Management
Technical Maturity

The vendor landscape for discovering and tracking the location of personal information is crowded, diverse, and confusing for healthcare industry buyers. Despite lots of tooling, only 17% of respondents are currently incorporating all five data types in their data privacy initiatives.

With so many DLP and other IT security vendors claiming to solve for regulations like the California Consumer Privacy Act, it's no wonder that respondents (90.48%) view these tools as helping them discover and track personal information. However, DLP is more about stopping insider threats and stopping end users from leaking out sensitive data (emailing it out).

63.41% of respondents reported using methods such as manually updated spreadsheets and surveys to track and inventory personal information while 62.50% rely on custom-written computer code.

What tools/software do you use to discover and track the location of personal information? Please select all that apply.
Surveys: Inaccurate and Time Consuming

Business Obligations

Regulations

Contracts

Internal

Challenges

- Point in time
- Doesn’t scale
- Evolving definition of PI
- Streaming data is blind spot

Unstructured File Shares
- Google Drive, Microsoft OneDrive

Structured Databases
- Oracle, MSSQL, MySQL, DB2

Big Data
- Hadoop, Snowflake

Additional Sources
- JDBC Connectors, RESTful API’s

SaaS
- Microsoft 0365, Salesforce

Data-in-Motion
- Kafka, Amazon Kinesis

Integris Software 2019 Data Privacy Maturity Study | Copyright 2019 Integris Software, Inc.
Data Privacy Management
Organizational Maturity

Organizational maturity for data privacy management is higher and more consistent than technical maturity.

91.30% of respondents had a data privacy and awareness program in place.

Does your current company have a data privacy training and awareness program?

- Yes: 91.30%
- No: 8.70%
Data Privacy Management
Organizational Maturity

78.05% had a process in place to evaluate the sensitivity of different datasets.

Does your current company have a process in place to evaluate the sensitivity of different data sets?

- **Yes**: 78.05%
- **No**: 21.95%
And 97.62% have a process in place to identify and mitigate privacy risk.
Data Privacy Management
Organizational Maturity

Organizations are also mature when it comes to handling customer consent, and communicating when things go wrong. 85% have policies, procedures, and mechanisms in place to track customer consent across channels.

Does your organization have policies, procedures, and mechanisms in place to track customer consent across channels?

- Yes: 85.00%
- No: 15.00%
Yet when technology is reintroduced to the equation, numbers begin to drop. 60% have an automated way to discover whose data was breached. Not surprising given the lower levels of data privacy technical maturity as reviewed in the previous section.
Data Privacy Management
Organizational Maturity

Data Privacy Team Size

An impressive 95.12% of respondents had data privacy teams in place, and over a quarter of respondents (26.83%) had data privacy teams of 25 or more.

How many employees are a part of your data privacy team? Note: Team can include full-time, part-time employees as well as consultants.

- We don’t have a data privacy team: 4.88%
- Less than 3: 4.88%
- 3 to less than 5: 24.39%
- 5 to less than 10: 21.95%
- 10 to less than 25: 17.07%
- 25 to less than 50: 9.76%
- 50 or more: 17.07%
Data Privacy Management
Organizational Maturity

Team Meeting Cadence

Almost a third of data privacy teams (28.27%) meet at least once a week. 41.46% admitted to meeting once a month or less. Infrequent collaboration could be a leading indicator to data privacy vulnerability, especially given that so many departments/roles have a stake in data privacy management.
International Regulatory Preparedness

Healthcare companies were best prepared for GDPR with 35.14% scoring themselves as Fully Prepared. No one scored themselves as unprepared.

Respondents were fully prepared for GDPR at much higher rates than the Australian (9.09%), Japanese (14.29%), and Chinese (14.29%) privacy laws. Levels of unpreparedness were also much higher here as well.
Domestic Regulatory Preparedness

Respondents appear to be behind when it comes to domestic regulatory preparedness. Only 16% said they were fully prepared for the California Consumer Privacy Act.
Perspectives

78.26% thought there should be a federal privacy law.

Do you think there should be a federal privacy law in the United States?

Yes: 78.26%
No: 6.52%
Unsure: 15.22%
Perspectives

80.43% of respondents thought businesses risk losing customers due to inadequate data privacy practices.

Do you think that businesses risk losing customers due to inadequate data privacy practices?

- Yes: 80.43%
- No: 15.22%
- Unsure: 04.35%

Integris Software 2019 Data Privacy Maturity Study | Copyright 2019 Integris Software, Inc.
Perspectives

And well over half (58.70%) thought that employers risk losing employees due to inadequate data privacy practices.
About Integris Software

Integris Software, the global leader in data privacy automation, helps enterprises discover and control the use of sensitive data in a way that protects privacy and fuels innovation. Regulations like GDPR and the California Consumer Privacy Act (CCPA) are triggering knee-jerk reactions as companies lock down their data for fear of misuse. Integris empowers security, privacy, and data governance leaders to make fact-based decisions about the use and transfer of customer data.

By working securely, at scale, no matter where data resides, Integris provides customers with an accurate and continuous picture of their data privacy landscape. With Integris, there is finally a way to use your data without fear.

For more information on Integris, visit www.integris.io or follow @Integrisio on Twitter.