COSMOS
Navigate the Compliance Universe

Compliance Today - May 2021
How effective information governance can help mitigate damages from an information breach

By Brian D. Annulis, Joseph Shepley, and Samir B. Almhiemid

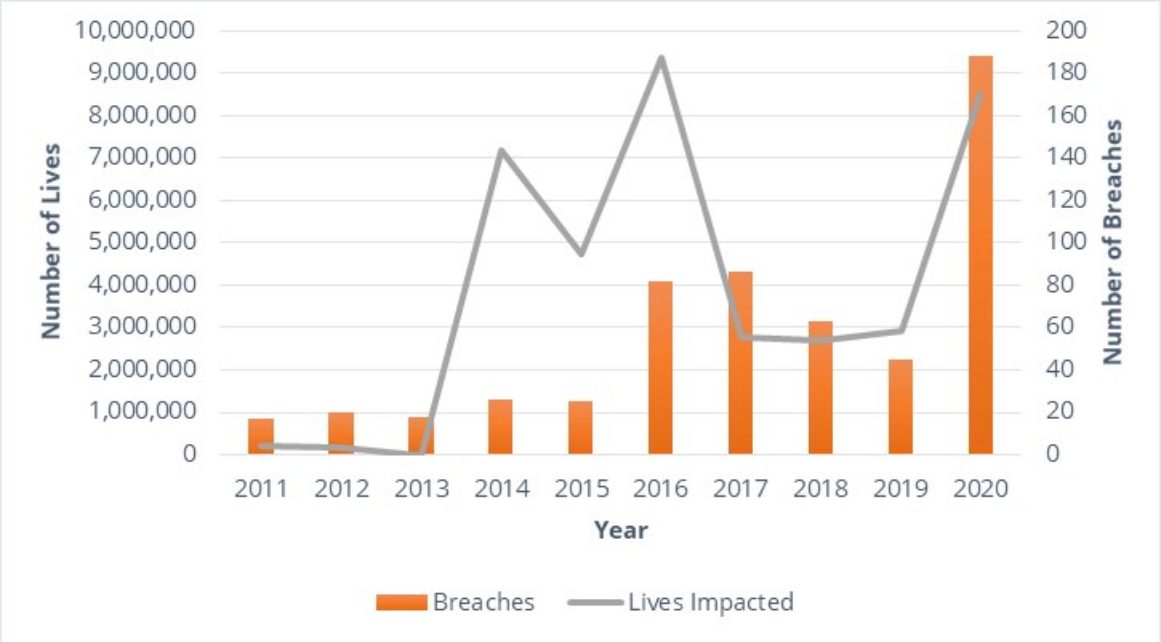
Brian D. Annulis (brian.annulis@ankura.com) is Senior Managing Director, **Joseph Shepley** (joseph.shepley@ankura.com) is Managing Director, and **Samir B. Almhiemid** (samir.almhiemid@ankura.com) is an Associate at Ankura Consulting Group LLC Chicago, IL.

- linkedin.com/in/brian-annulis-71195b1/
- linkedin.com/in/joeshepley/
- linkedin.com/in/samir-almhiemid-aa8337157/

Healthcare organizations today face unprecedented challenges managing and protecting their sensitive electronic information—not only electronic protected health information (ePHI) but other high-value, high-risk data such as personally identifiable information (PII), payment card industry (PCI), network access credentials, and financial data. Prior to 2020, cyberattacks had been on a steady year-over-year increase, but in 2020, this steady increase turned into explosive growth.

Healthcare experienced a more than 9,000% increase in endpoint attacks compared to 2019, which led to approximately 1 million patient records breached per month.[1] The U.S. Department of Health & Human Services Office for Civil Rights (OCR) breach data[2] shown in Figure 1 tells a similarly alarming story: in 2020, there were 188 reported breaches of network servers[3] involving 500 or more individuals—a more than 400% increase compared to 2019 and a more than 200% increase compared to 2017, which was the previous high-water mark for reported network server breaches. Beyond the typical impacts of these attacks, such as regulatory fines, sanctions, and mandated corrective action plans, 2020 also saw the first-ever reported loss of life due to a cyberattack: in September, a German patient died during a ransomware attack when being rerouted to another healthcare facility to receive care.[4]

Figure 1: Number of breaches and lives affected 2011–2020



Cybersecurity is not enough

In response to the increase in cyberthreats, healthcare organizations have quite rightly focused on their cyber defenses: hardening their endpoints (e.g., laptops, mobile devices, and web applications); strengthening their network access credentials (by introducing two-factor authentication, requiring more frequent password updates, and removing outdated or expired credentials); and more actively and closely scrutinizing the security posture of third parties (such as vendors, contractors, and other partners).

Yet, as important as these cybersecurity-focused efforts are, the reality is that no organization can prevent all breaches; no matter how much time or money is applied to cybersecurity, there will inevitably be breaches. Regrettably, when it comes to being a victim of a cyberattack, it is a matter of when, not if.

This somber reality means that healthcare organizations, to better address the heightened levels of risk in our new normal, need to complement their cybersecurity-focused efforts with information governance (IG) efforts to help them better manage the information (sensitive or otherwise) behind their firewall. When done properly, IG will help ensure that when the next breach happens—which it will—the attackers will find less sensitive information to compromise, and the organization affected will have better (and more rapid) visibility into what information was in fact compromised.

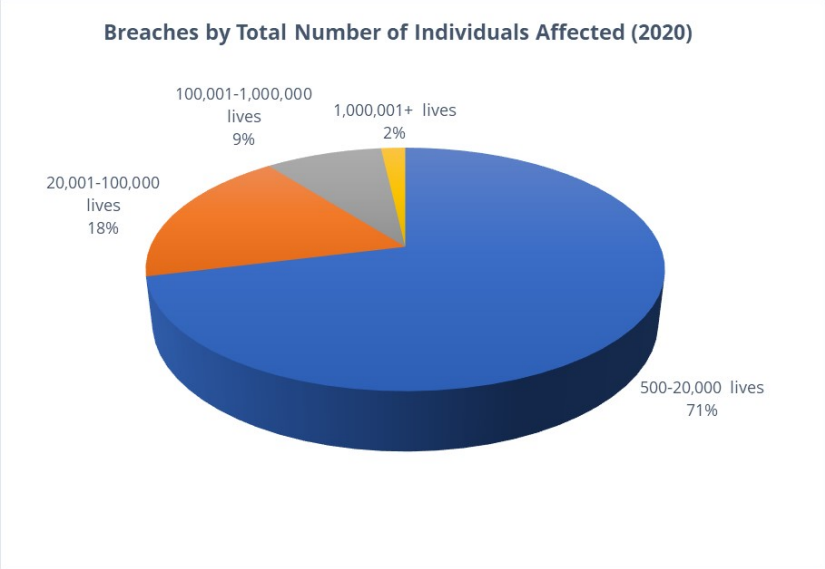
The IG problem in healthcare

Despite the increase in threats to healthcare information seen in 2020, IG has been a challenge to implement in healthcare (as in most industries) for a long time now. The proliferation of systems, storage locations, and methods of creating and sharing electronic information across the organization and with third parties has made governing information difficult. Simply knowing what information is stored where, of what kind, and accessed by and shared with whom is a significant challenge for most healthcare organizations—let alone managing that information systematically, consistently, and transparently to comply with organizational policies, contracts, laws, and regulations.

And the failure to do so brings with it the risk of significant fines and sanctions. According to IBM, the average overall cost of a healthcare breach was more than $7 million in 2020,[5] while the average OCR fine per health

record breached in 2019 was $429.[6] Given the number of health records involved per breach in 2020 (as shown in Figure 2),[7] nearly 30% of the breaches would have surpassed the $7 million figure in fines alone, not including the other costs associated with a breach, such as cyber-remediation, legal fees, public relations management, and regulatory compliance management. Although the Fifth Circuit Court of Appeals' recent decision in the MD Anderson case[8] offers hope to Health Insurance Portability and Accountability Act covered entities and business associates in regard to the range of reasonable fines and penalties for breaches, significant fines and penalties are still possible if not probable.

Figure 2: Breaches by total number of individuals affected



A framework for IG in healthcare

Given the threat landscape for healthcare organizations and the importance of IG as a complement to cyber-focused efforts to protect sensitive information—and given how challenging IG has been historically for many healthcare organizations—what is the best way to develop the IG capabilities required to effectively protect a healthcare organization's sensitive information?

In our experience, good IG is like getting healthy: the basic principles (sleep, eat right, stay active) are straightforward, but adopting those principles and living them day in, day out (implementation) is a challenge, as shown by the spike in gym memberships every January and the steady drop in gym attendance every February.

In order to properly protect ePHI and other high-risk information (as well as pruning it for stale, junk, and duplicate information), there are three core, best-practice IG principles that are absolutely critical for healthcare organizations, regardless of size:

1. Keep information only as long as legally or operationally required, then dispose of it;
2. Dispose of information using a policy-driven, repeatable, and consistent process; and
3. Monitor information disposal regularly.

Figure 3: Key questions for good IG

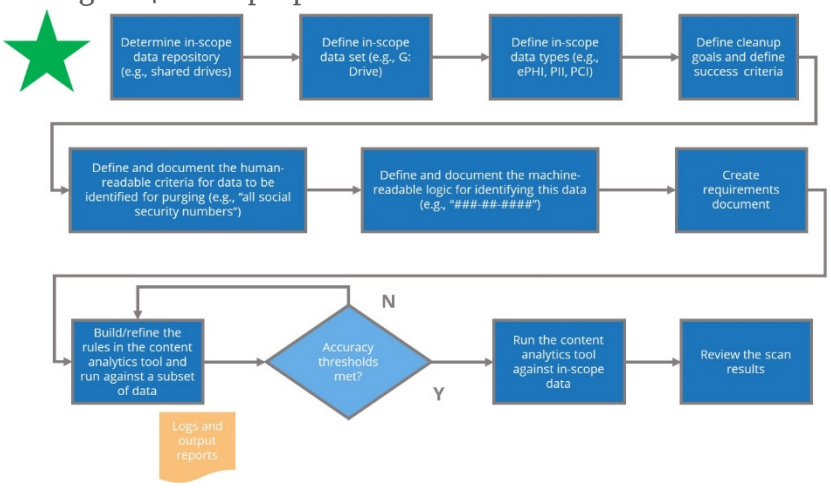
Keep data only as long as legally or operationally required – then dispose	Dispose data using a policy driven, repeatable, and consistent process	Monitor data disposition regularly
• Is it on legal hold? • Is it subject to regulatory or other preservation obligations? • Are there legitimate business reasons for keeping the data?	• Are there policies in place that address managing data throughout its lifecycle? • Information Governance, Data Management, Records Management, Legal hold/eDiscovery, Orphaned Data, etc.? • Do they apply to everyone who works with data (e.g., employees, contractors, vendors, etc.)? • Are there processes and guidelines to direct process participants? • Is there technology in place to perform file analytics, disposition workflow, purging, etc.?	• Are there logs of data purged and "certificates of destruction" (or equivalent)? • Are records of end user training kept? • Are there certifications from data owners and custodians of compliance? • Are reports of data volume trends by type (e.g., growth of or reduction in sensitive, junk, stale, etc.) available?

And as with getting healthy, as straightforward as these core principles seem to be at first glance, living up to them (i.e., implementing them) can be difficult. Figure 3 presents some of the key questions you need to ask to determine whether your organization is ready to adopt these core IG principles and better protect your sensitive information.

Principle one

Your ability to confidently answer the questions related to the first principle and dispose of data after they are past their legal and operational life relies primarily on *knowing what kind of information is stored in each corporate system.* And this knowledge shouldn't simply be based on what corporate policies or procedures say is the case, what system or data owners tell you through surveys or interviews, or what other second-hand, top-down channels convey (as important as they all are for your IG efforts); rather, to get a more direct line of sight on your information and manage it properly, you need to analyze your information at the file level, assisted by technology, to provide you with data points to determine (to an acceptable level of certainty) whether that information is junk, stale, duplicate, sensitive, or risky. A sample process for information identification is shown in Figure 4.

Figure 4: Example process for information identification



Regardless of the specific process you use to identify your information, once you gain visibility on what kind of information you have and where, you can begin your efforts to practice good IG.

Principle two

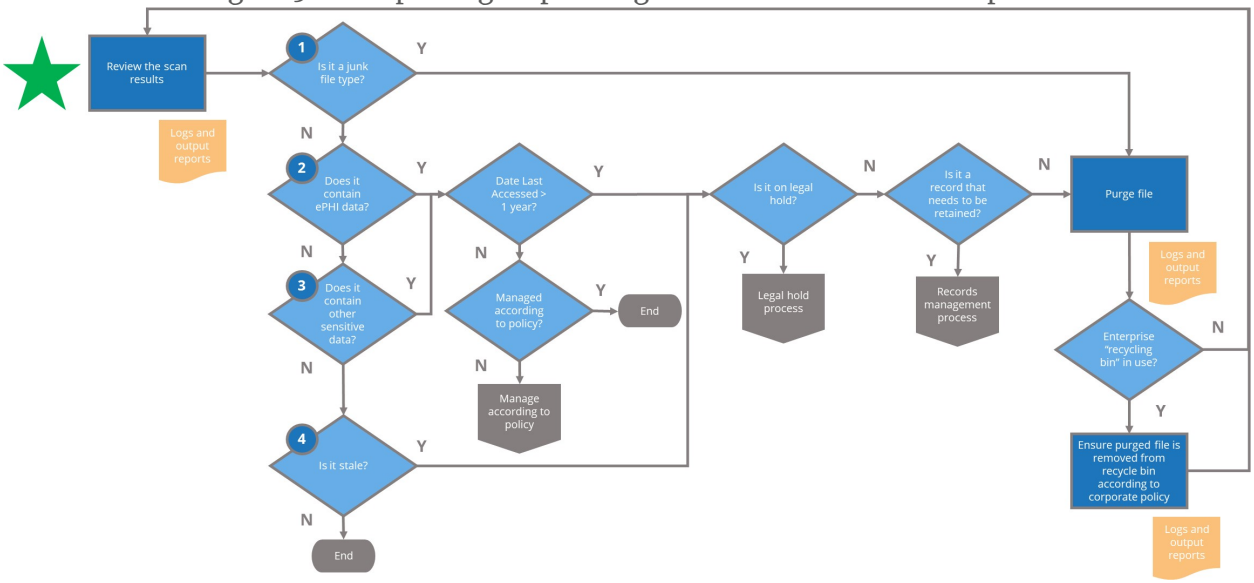
Management of activities at your organization that are subject to laws, regulations, contracts, or other obligations should be policy driven, repeatable, and consistent—and IG is no exception. And although the specific obligations that affect IG will differ from organization to organization in healthcare, they go far beyond those related narrowly to OCR to include obligations related to the Federal Rules of Civil Procedure, the Food and Drug Administration, the Occupational Safety and Health Administration, the Federal Trade Commission, state insurance departments, organizations like the American Medical Association, and specific privacy regulations (e.g., the California Consumer Privacy Act or the European Union's General Data Protection Regulation), among others.

And while it is beyond the scope of this article to present a comprehensive policy framework for healthcare information management compliance, typically the following structure is a good practice that enables the kind of policy-driven, repeatable, and auditable processes—for IG or otherwise—we are advocating here:

- **Policy**: Contains what an organization will do to meet its obligation(s),
- **Procedure**: Contains how an organization will accomplish the "what" in a policy, and
- **Guideline**: Contains how an individual will execute the steps in a procedure to accomplish the "what" in a policy.

Once your organization has these three levels in place for IG, the process for managing information to reduce risk can be codified in a target operating model (TOM) such as the example shown in Figure 5.

Figure 5: Example target operating model for information disposal



Although in actual practice a TOM for IG at a healthcare organization would be far more complex, the basics are the same: to enable effective IG, the TOM must indicate how to handle information that:

1. Has no value to the organization (aka "junk data");
2. Contains ePHI;
3. Contains other sensitive data (e.g., PII, PCI, network credentials, etc.); and

4. Is stale (e.g., has not been accessed in a certain number of years).

In addition, a TOM for IG must account for, at a minimum, compliance with legal/litigation holds and corporate record-keeping requirements; beyond that, compliance with other obligations can be included in the TOM at relevant points in the process (e.g., after determining date last accessed or confirming a legal hold).

Principle three

Once a healthcare organization has implemented an IG program, employees, contractors, and other third parties need to comply with the program's requirements, particularly those relating to data retention and disposal. As with any effective compliance program, monitoring adherence to applicable IG policies, procedures, and guidelines is essential, not only for demonstrating compliance in response to requests from regulators, courts, and other authorities, but for enabling better information management by end users and your organization in general.

To that end, it is critical for a healthcare organization (i.e., its compliance or internal audit department) to routinely monitor and audit whether the organization is consistently managing its information according to policy, from creation to disposal, regardless of whether the information is considered junk or stale, on the one hand, or sensitive (e.g., ePHI, PII, PCI) on the other. And because the goal of monitoring is to enable continuous improvement, an organization needs to take a long hard look at the results of monitoring to determine the root cause of deficiencies (e.g., policy or procedure gaps, implementation issues, end-user training), define a remediation plan to address deficiencies, and then work the plan, monitoring at every step to ensure that deficiencies are indeed being remediated and IG is improving accordingly.

Conclusion

So, what is the next step in implementing an effective IG program? Begin by asking the following questions:

- Do you know how much ePHI (or other sensitive information) is stored on your organization's network and how it is being managed?
- Do you have technology capabilities to identify and secure ePHI on your organization's network in a cost-efficient, sustainable way?
- Do you have agreement from key organizational stakeholders on how to manage ePHI that has been orphaned and abandoned?
- Do you have compliance controls in place to enable managing uncontrolled ePHI on your organization's network?

Satisfactory resolution of these issues will go a long way toward putting your organization on the right path for an effective IG program—one that helps you mitigate the risks associated with a security incident or breach.

Takeaways

- Become an information governance (IG) resource: Learn all you can not only about the state of IG at your organization but about the state of IG in industry. What are other healthcare organizations doing? What does good IG look like according to those who know? What are some key practices and concepts that could help your organization?
- Become an IG evangelist: Share your IG knowledge with your organization to find others who are willing to

become IG stakeholders and contribute to your efforts.

- Get the conversation started: Work to create dialogue and communication among the IG stakeholders at your organization so that key IG issues are raised and discussed.
- Create a community: Find ways (both formal and informal) to build a community of IG stakeholders at your organization and use that to support IG efforts.
- Adopt a vision: Leverage the community of IG stakeholders to articulate a vision for IG at your organization that will foster more effective management of information to reduce its risk and increase its value.

1 Steve Alder, "VMWare Carbon Black Explores the State of Healthcare Cybersecurity in 2020," HIPAA Journal, February 8, 2021, http://bit.ly/3f0K0vN.
2 "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," Office for Civil Rights, U.S. Department of Health and Human Services, accessed March 17, 2021, http://bit.ly/38UxxpM.
3 45 C.F.R. § 164.402 .
4 Melissa Eddy and Nicole Perlroth, "Cyber Attack Suspected in German Woman's Death," *The New York Times*, September 18, 2020, http://nyti.ms/2P702MA.
5 IBM Security and the Ponemon Institute, *Cost of a Data Breach Report 2020* , accessed March 17, 2021, http://ibm.co/3bYTeHb.
6 IBM Security and the Ponemon Institute, *Cost of a Data Breach Report 2019* , accessed March 17, 2021, http://ibm.co/38QGm3P.
7 "Breach Portal," Office for Civil Rights, U.S. Department of Health and Human Services.
8 Theresa Defino, "HIPAA News: MD Anderson Avoids $4.3M Fine, New Law Ties Penalties to Compliance Efforts," *Report on Research Compliance* 18, no. 2 (January 20, 2021), http://bit.ly/3qX6yQo.