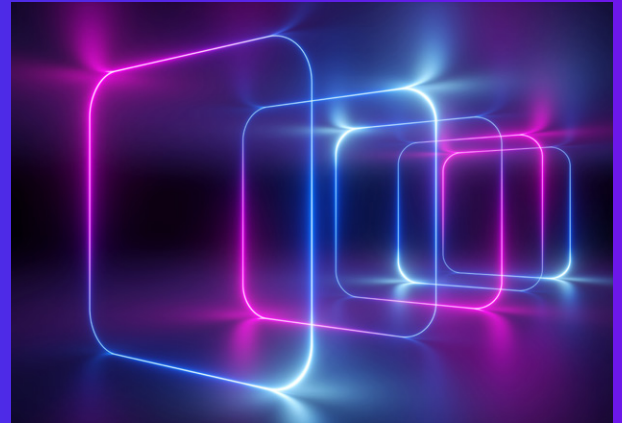




# De-mystify the de-identification of sensitive patient data

By Randall Walker



For healthcare organizations, protecting and managing sensitive patient information is a way of life. Local, regional, and global restrictions and regulations have rightly become more and more strict to protect patient rights. But unlocking the full potential of this collected data has huge value for clinical trials, research, and other cross-organizational activities.

For most healthcare organizations, the challenge comes from seamlessly sharing data between entities without violating the need for privacy. Today's cloud computing environment makes this easier, but the task of masking confidential patient information is still an onerous one. Often, the burden of ensuring privacy is placed on hospital and provider staff as part of their day-to-day jobs—taking them away from patient care and even life-saving activities.

Leveraging existing technologies such as Google Cloud de-identification tools provides some real help in this area—both for those new to the cloud and for organizations with established cloud environments. You can avoid building programs from scratch and enable them to access sensitive data without the risk of exposure.

KPMG has helped many clients use the Google Cloud environment. For those new to cloud, one option some choose is to begin by using data transformation and migration to mask sensitive data so that they can get enough content to support their solution through development. Google Cloud tools can ingest the data once obfuscated on premise through batch job—or as part of a near real-time streaming service.

For those already in a cloud environment who want to broaden their ability to share more complex information, such as imaging, the full suite of Google Cloud de-identification tools is available. You can automate content de-identification based on levels and specifications. These tools can help with a myriad of options ranging from redactions to specific

de-identification rules that can be applied across multiple types of documents. Automation can process content and place it in secure cloud sub-environments (Service Projects) where third parties can either access it, or it can be sent per your specifications.

The big advantage? *Time*. A good amount of time can be saved that is currently being spent on manually de-identifying records. And that will help free up more resources for patient care and problem solving.

Another big advantage of automating this process is the ability to quickly identify patients who qualify for trials. It eliminates the need for manual searches and dramatically enhances the ability to improve accuracy and the effectiveness of treatments and protocols. Information is stored in one central repository, providing more context about the patients.

For those wanting to embark on this journey, the rewards are great. To make the process go smoothly, it helps to have the advice of people who understand healthcare as well as data engineering and the technology that's required to configure it. KPMG brings all this along with an abundance of experience using Google Cloud solutions.

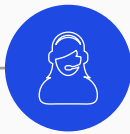
We don't start with technology. We begin with understanding the problems our clients want to solve, then translate that into a meaningful solution. We sit with health care providers to understand the scenarios they face. We also work with the primary investigators who manage clinical trials to understand their needs for information. Then we configure the technology to work for both parties.

We also understand the necessity for security, audits, controls, and log monitoring so information can be traced and accessed by only those with specific rights and needs to that data. And if a broader approach to security is required for the environment as a whole, we understand what is needed to do that efficiently. We've built a HIPAA-compliant, automated environment in our own company to ensure it meets all privacy requirements.

It's important to use a holistic approach when building a de-identification solution. It should consider all the issues and needs of both healthcare providers and end users and be flexible enough to meet them. Being thorough in design means avoid creating solutions that ultimately cause problems in other areas. For example, you want to:



Define the benefits for your organization



Assess whether or not you have the right staff to support the solution



Understand how other applications use your solution



Determine how source systems will be impacted by integrating with your solution



Map out how the changes you make to the data through your solution will impact your organization's overall data management and governance strategy



Think about your long-term goals, and how those might be integrated in what you are doing today

It takes the type of collaboration that KPMG is well versed in. With KPMG and Google Cloud, you can gain the confidence to apply automation and a modernized approach to your de-identification challenges and support your team for long-term success. Ultimately, the greatest benefit lies in creating better patient outcomes.

If you would like to know more about how we can help, please contact me.

## Contact us



**Mike Krajecki**  
**Partner, Advisory**  
KPMG LLP  
**C:** 847-707-7689  
**E:** mkrajecki@kpmg.com



**Randall Walker**  
**Director, Advisory**  
KPMG LLP  
**C:** 678-637-5572  
**E:** randallwalker@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS005411-2A

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.