wiley

NEWSLETTER

Employer Challenges for Health Care Data Are Growing

March 2018

Privacy in Focus®

For reasons largely lost to American history, for many decades employers in the United States have been intimately involved in the provision of health care services – including health insurance – for their employees. While the role of employers in providing health insurance is the source of extensive debate today, a substantial portion of Americans continue to receive their health insurance coverage through their employer.

Obviously, as with everything in the health care system, the role of employers has been evolving in recent years. Many employers still provide on-site health clinics for their workers, which may provide a broader range of services than just routine care in connection with work-related activities. Employers are struggling to make health care and health insurance programs both more effective in promoting employee health and less expensive. The industry saw enormous speculation about the potential impact of a recently announced partnership between Amazon, Berkshire Hathaway, and J.P. Morgan to engage in some new form of employee health care and health insurance (although details are scarce).

The general push towards wellness programs also has complicated this discussion. As employers (and the vendors they retain to promote these programs) expand wellness programs, both in terms of scope and potential impact on employees – employers are faced with increasing challenges in terms of how to realistically, effectively, and appropriately monitor and oversee both these programs and their employees' health in general.

Practice Areas

Privacy, Cyber & Data Governance

Most recently, Chrissy Farr, CNBC's prominent and tireless health care and technology reporter, reported on an intriguing new development involving Apple, where Apple has announced that it will be establishing primary care clinics for some of its employees (starting near its corporate headquarters). While described in these reports as "independent of Apple," these clinics will create more tensions for the employer's role in providing health care services for employees because of the volume of health care data that will be gathered.

On top of all these challenges are the HIPAA privacy and security rules, which create compliance challenges for any employer that provides health insurance benefits to its employees.

So, with that background, what should employers be paying particular attention to in connection with their provision of health care services and related benefits to employees?

HIPAA compliance is even more important in today's environment

Since the HIPAA privacy rule first went into effect in 2003, employer health plans have been "covered entities." While this may have been an odd result, and employer health plans never operated in the same way as a hospital or health insurer, the rules applied to these plans. I first wrote about these obligations in 2004, in an article entitled "Making Sense of HIPAA Privacy for Employers." (An updated version of this article is available here.)

Now, almost 15 years later, it continues to be surprising to me how few employers seem to understand that they are subject to HIPAA if they provide health care benefits to employees, and how many of those that are aware of these obligations have not re-evaluated their compliance activities in many years. For most employers, these obligations arise because the employee benefit plan that provides health insurance benefits is considered a "health plan" under the HIPAA rules. The company's obligations will vary somewhat based on how the plan is financed and operated. And some of the risks I was concerned about in 2004 have not in fact arisen (such as the likelihood that employees who were terminated would allege HIPAA-related violations which could create problems for employers even where none should exist because of a failure to comply with HIPAA's regulatory requirements).

Other employers – a smaller number for sure – may also have obligations as a health care provider, if health care services are provided directly to employees in certain situations.

But the fact remains that employers in every industry need to evaluate their HIPAA obligations and take steps to both comply with the rules (based on the enforcement and security breach risks) and ensure that sensitive employee health information remains appropriately protected.

HIPAA creates two major challenges for employers. First, from the employee benefits perspective, HIPAA imposes compliance obligations on the benefit plan directly – not on the employer. However, this obligation does not reflect the reality at most employers – which is that the benefit plan is primarily a contract with employees that is defined by the ERISA statute and is not in any other way an independent organization or group of individuals. Employers must make sense of how to comply with a set of obligations imposed on this

piece of paper.

In addition, the HIPAA rules do not apply to all health information – they apply to individually identifiable health information in contexts subject to the HIPAA rules, mainly where a health care provider or health plan is involved. So, there is a broad variety of "health information" held by employers – from workers compensation and disability claims to Family and Medical Leave Act materials to basic employment-related data – which is health-related but is not subject to the HIPAA rules.

A few key steps that virtually any employer should be taking:

- You should be conducting a review of the role played by your company in the management of your health care benefits program.
- You should identify the information that comes into your company that is regulated by the HIPAA rules – primarily the information about employee health care claims through your health insurance benefits program.
- You should identify (and strictly limit) the internal personnel who play any role in the use or disclosure of individually identifiable health information from your benefits program.
- You should train these people on the requirements of the HIPAA rules and the complexity of overall management of employee health data.
- You should identify where within your information systems this individually identifiable health information is stored.
- You should conduct a security risk assessment for those information systems that store this information.
- You should evaluate the overall requirements under HIPAA for documentation of your HIPAA obligations, and evaluate carefully whether your policies and procedures meet these requirements.
- You should have a plan for how to separate HIPAA data from other employee data.

Understand your wellness program

The complexity of HIPAA's requirements in an employer-based environment is exacerbated by the recent expansion of employer wellness programs, which raise both the confusion and risks related to the protection of employee health information.

Wellness programs are evolving constantly. There is a meaningful debate about whether these programs are "successful" (including debate on how to measure what successful means). Early programs were often informational – simply providing information about specific illnesses or conditions (e.g., smoking cessation) to whomever was interested in receiving it. Now, these programs are often more participatory – and significantly more information is gathered through them. They often involve a requirement to participate in certain health insurance programs, or provide discounts (or penalties) based on your participation. Other programs focus on substance beyond "participation," to include actual results.

For employers, it is critical to understand how these programs operate, even if you have primarily outsourced their operation. Are they covered by HIPAA? This may depend in large part on who is covered by them – if employees who are not part of your health insurance program can participate in wellness programs, then HIPAA may not be relevant. If HIPAA is not in play, what are the guiding rules? Do you know what your vendor is doing with information about your employees? Do the employees know? Has someone provided them with a privacy notice about the wellness programs? Do they have reasonable choices about the information being collected and how it is being used?

These wellness programs are complicated, and may present opportunities to control costs through improved employee health (presumably a win-win). There certainly are those in the field who believe that wellness programs disproportionately focus on costs without addressing employee health. Independent of this debate, companies that offer wellness programs should ensure that they understand how they operate, are aware of how employee data is being used and disclosed (and by whom), and that employee privacy issues are being considered appropriately in the management and oversight of these programs.

Employee monitoring should be included as well

An additional (and increasingly important) element is overall employee monitoring and related data gathering efforts by employers. This is a particularly challenging area because it is very loosely defined. Employers are looking constantly to improve employee performance. This effort is taking on a growing range of possibilities because of new means of overseeing what employees are doing on the job, and new areas where employers can gather data about what employees are doing away from the job.

From a privacy perspective, the biggest risk for employers may be in gathering and analyzing data without a thoughtful privacy analysis upfront. Because of the significant gaps in the law that exist today (for example, in the collection of health data outside of the HIPAA environment), companies may in fact have reasonable flexibility to gather and analyze data about their employees. At the same time, there are substantial risks that can be avoided through thoughtful planning.

Do you know what data you have about employees? Conduct a thoughtful review throughout your company on where data about employees is being collected – and make sure that you update this regularly, as your corporate team will be looking constantly for new sources of information.

Do you know how this information is being used? Are you making judgments about employees based on this information? Do employees know this? Do you have standards for how to make these decisions?

Have you restricted where this information goes and who has access to it?

Have you implemented reasonable and appropriate security procedures for any portions of your information systems that store this information? Remember – even if HIPAA is not relevant, many state laws now require breach notification in the event of security breaches involving health information.

Do you have documented procedures about this information, including when it is covered by HIPAA, when it is not, and how you are keeping those lines separate?

Managing Your Contracts

Many of these information-gathering efforts are operated by outside entities – the sources of much of this information, the operators of various programs, and the analytics firms that guide decision-making. Do you have appropriate protections – for your employees and your company – in these contracts? Do you know what these companies are doing with data about your employees? What happens if there is a security breach on their end about this information? Make sure that your contracts address these issues and that they stay current as laws and practices evolve.

Do you have an international component?

The HIPAA rules and state breach notification laws create enormous tensions and complexity for employers operating in the United States. Do you have an international component that adds to these concerns? New data protection laws across the globe are expanding on these challenges. The new GDPR rules going into effect in Europe later this year (May 2018) will create compliance challenges for a broad range of companies, both obvious ones operating in the EU and many others. If you have employees in other countries – particularly in Europe – and you send employee data to the United States, you will need to meet both the compliance challenges of the law where the data starts (in Europe, the GDPR, for example), as well as the array of new data transfer principles that you must meet to legally transfer data from these countries to the United States (such as the Privacy Shield program or the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System). For many of these countries, health data is considered sensitive data, with additional compliance obligations and complications.

Do you understand the scope of health data?

Last, one of the most recent developments in the broadest health care privacy space involves the increasing breadth of the personal data that is considered "health data," or that is being used for health-related purposes. Insurers are using data such as income, marital status, and number of cars to evaluate potential emergency room utilization. Health care providers may be taking action based on patient data involving clothing purchases and gym membership status. As new sources of data emerge, data analytics professionals (who operate in a very loosely regulated environment) search for meaningful connections between pieces of data and intended results. They often want data simply to evaluate where it might be relevant or how it could be used – without any real sense of how useful or accurate it will be. You should understand how your company – and your vendors – are gathering and using data about your employees, to understand whether these actions create meaningful privacy concerns.

Have you communicated to your employees?

Privacy notices remain an important element of how any company communicates its data use activities to its relevant audiences, and how it also protects itself from allegations about its activities. Outside of HIPAA (for employers), many privacy notices are not heavily regulated, or there is substantial flexibility to describe comprehensively and accurately how a company is using data. Any employer should be re-evaluating its employee privacy notices, to ensure that it is incorporating all relevant activities and uses of the data.

Conclusions

Personal health care information is inherently sensitive. And, while the scope of what is considered health information is growing, individuals remain concerned about job impacts, personal embarrassment, insurance risks, and a broad variety of other potential risks of adverse consequences resulting from their health care information. Identity thieves also find health care information to be incredibly valuable. At the same time, as employers become more involved in the overall management of employee wellness and health care expenditures, there is a stronger interest in effective management and utilization of this employee data for a growing range of employer interests. And, as employers participate (along with many others) in the big data revolution, there are new opportunities to gather information that will promote more effective and efficient workplaces. Employers need to very carefully consider their approach to employee health care information and how they will act effectively and intelligently in this controversial and risky area. This is not a message to avoid this data or avoid its potential benefits. Instead, the challenge is to ensure that you are engaging in this growing range of opportunities with careful thought and an appropriate consideration of the evolving and confusing legal and regulatory environment.