Various federal laws govern wellness programs, including Title I of the Americans with Disabilities Act (the "ADA"), Title II of the Genetic Information Nondiscrimination Act ("GINA"), and the Health Insurance Portability and Accountability Act ("HIPAA"). These statutes require employers to maintain their employees' health-related information in a confidential manner.

In general, employers' wellness programs can collect any health information from employees. Although the ADA and GINA generally prohibit employers from collecting health information from their employees, both statutes provide exceptions for voluntary wellness programs. In fact, recent rules promulgated by the Equal Employment Opportunity Commission regarding ADA and GINA explicitly chose not to restrict wellness programs from collecting only the minimum necessary health or genetic information to directly support program activities. There are limitations, however. For example, under ADA, employers must make the programs voluntary, keep the information confidential and separate from other employee records, and not use the health information as the basis of employment decisions. Similarly, under GINA, employers must make the wellness programs voluntary, and employers cannot require that employees provide their genetic information as a condition to receiving incentives. Further, employers must obtain written authorization from the participating employees that the wellness program's policy: (1) is written in a manner that the employee is reasonably likely to understand it; (2) describes the type of genetic information that will be obtained and how it will be used; and (3) describes the restrictions on the disclosure of genetic information.

With respect to vendors, they generally may sell the health information they collect through wellness programs. Although HIPAA protects individually identifiable health information, this information must be created or maintained by health plans and health care providers. Because most vendors are not connected with health plans, HIPAA does not apply. Employers could always limit the sale of such information through contract, however.

Robert Gilmore, Partner, KJK

Employers have been buying a number of "plug and play" solutions to improve the health and wellness of their populations. In order for these programs to be successful, we generally believe that vendor access to employees information such as name, address, email address and telephone numbers is critical. Many employers lack that information or refuse to release it to vendors. When vendors propose purchasing data in the marketplace, employers often say no due to HIPAA or State privacy law concerns. Are they being overly cautious? There is no blanket answer, but there are factors to consider.

First off, the elephant in the room is the potential for huge HIPAA penalties. HIPAA regulations state that the penalty for each violation may not be more than $50,000, or more than $1,500,000 for identical violations during a calendar year, even if it is established that the entity "did not know and, by exercising reasonable diligence, would not have known …" that it violated the law. Each day of noncompliance may be a new "violation." Penalties are greater in other circumstances.

But is an employee's name, address or phone number protected health information? If it is PHI, remember that all disclosure is prohibited unless specifically permitted.

Analyzing disclosures is very fact specific, and the views of practitioners vary, so answer these questions: (1) Is a health plan involved so that HIPAA is relevant? (2) Is the information PHI? PHI includes (among other things) any information received by a health plan or employer that relates to the future health of an individual or payment for health care and identifies or could be used to identify the individual. (3) Is its disclosure permitted (i.e., is it for treatment, payment or health care operations)? (4) Is the disclosure only the "minimum necessary" information. (5) Does the disclosure violate what you have said in your Notice of Privacy Practices, SPD or HIPAA Policies and Procedures? (6) Have you documented the reasons for any disclosures that might be questioned? (7) Finally, have you negotiated adequate insurance coverage and vendor indemnifications?

For further information, visit the Office for Civil Rights website. While you are at it, follow the link below to a HIPAA parody of Michael Jackson's Thriller video – suitable for the Halloween season.
https://www.youtube.com/watch?v=dahpWh5ttCw

Ronald Stansbury, Attorney, Tucker Ellis LLP

In general, employers are permitted to collect information from their employees as part of the hiring process provided that requesting the information is not otherwise prohibited by law. As a result, employers typically gather contact information, addresses, phone numbers, email addresses and other information based on legitimate business needs of their organization.

Due to the uptick in identity theft issues, employees have become more concerned about the disclosure of certain information with anyone outside the employment relationship. Given the identity theft concern, numerous states have restricted how employers may use personally identifying information such as social security numbers and dates of birth. Other states have extended these protections to other types of information, including home address, telephone numbers and personal email addresses. In New York, for example, such information is defined as "personally identifying information," and may not be posted, displayed or communicated to the general public. N.Y. Lab. Law Sec. 203-d(3). Although many jurisdictions do not limit the use of such basic contact information, more and more states are considering ways to further protect employee privacy. As a result, the best practice is to seek employee consent before releasing such information.
If the information is collected by the employer's group health plan, it is most likely protected health information (PHI) and is protected by the Health Insurance Portability and Accountability Act (HIPAA). As long as the health plan has a business associate agreement with the vendor, PHI can be disclosed to the vendor without the employee's authorization for health care operations, including to administer a wellness program. Whether the information is collected by the employer or the group health plan, employers should ensure that any disclosure is not in violation of applicable law and that any vendor agrees to maintain the confidentiality of the information disclosed.

Stephen Penrod, Attorney, Thompson Hine LLC