To Clients and Friends **January 2008**

STATES EXPAND DATA BREACH STATUTES TO APPLY TO MEDICAL INFORMATION

To-date over 35 jurisdictions have enacted data breach notification statutes requiring businesses to notify consumers, and in some instances state agencies and the credit reporting agencies, in the event that an unauthorized person obtains access to a consumer's "personal information." Recently, California joined the ranks of a minority of states whose statutes specifically define personal information to include medical information.

1. Health Care Providers' Obligation to Protect Patient Information.

For medical providers, the Health Insurance Portability and Accountability Act ("HIPAA") is the most well-known source for rules and regulations concerning the protection of patients' medical information. HIPAA is not the only data-security legislation applicable to health care providers. HIPAA allows states to enact additional legislation to further protect patient confidentiality and privacy.

2. State Statutes Generally Require that Consumers Be Notified if Their Personal Information Is Accessed by an Unauthorized Party.

The vast majority of state data breach notification statutes apply to health care providers. Under most state data breach notification statutes physicians, hospitals, and insurers must alert their patients only if the patient's name and social security number, drivers license number, or financial account number, is disclosed to an unauthorized third party, however. Most states do not require that a provider alert a patient if only the patient's medical information, and not the patient's other information, is disclosed to an unauthorized party.

3. Some States Have Expanded Statutes to Explicitly Cover Health Related Information.

California recently joined Arkansas in defining "personal information" under its data breach notification statute to include "medical information" such as a patient's medical history, mental or physical condition, or medical treatment or diagnosis. California has further expanded the definition of "personal information" to include consumers' health insurance policy numbers and subscriber identification numbers. Other states, such as Nebraska and Wisconsin have expanded their statutes to include a much narrower category of health related information – biometric data – which includes such things as DNA. As a practical matter this means that a provider may have to alert a patient if medical information is breached, even if that information does not include a social security number, drivers license number, or financial account number.

4. How Can Providers Comply With Data Notification Laws?

Hospitals, insurers, and physicians, have a wealth of information relating to their patients and employees. Not surprisingly, over the past two years the health care industry has been one of the largest sources for data breaches.

Bryan Cave's Privacy and Information Security Team has extensive experience designing *comprehensive* data-security programs. The precise contours of a "comprehensive" data-security program depends upon correctly identifying all of the laws, including state data breach notification laws, to which you may be subject. Any security program should, however

- Designate an employee to coordinate an information security program;
- Identify reasonably foreseeable internal and external risks to security;
- Assure that contractors are capable of maintaining appropriate safeguards;
- Continually be evaluated (and reevaluated) to reflect new circumstances;
- Provide consumer notification plans in case of an inadvertent data-security breach.

5. What Should I Do If a Data-Security Breach Occurs?

Act immediately to prevent liability. Bryan Cave's Privacy and Information Security Team can quickly respond to data-security breaches by identifying applicable notification requirements under various federal and states laws and designing appropriate consumer and governmental agency notifications.

* * *

If you would like further information on how our experience can provide unparalleled insight before, and after, a data-security breach please contact any of the following attorneys:

Washington, D.C.

Jodie Bernstein
(202) 508-6031
jzbernstein@bryancave.com

Dana Rosenfeld
(202) 508-6032
dbrosenfeld@bryancave.com

David Zetoony
(602) 364-7142
david.zetoony@bryancave.com

Jill Zucker
(202) 508-6122
jmzucker@bryancave.com

New York

Joe Sanscrainte
(212) 541-2045
New York, NY
joseph.Sanscrainte@bryancave.com

Missouri

Karen Garrett
(816) 374-3290
Kansas City, MO
klgarrett@bryancave.com

Kathleen Reardon
(314) 259-2269
St. Louis, MO
kcreardon@bryancave.com