Robert P. Giacalone
Senior Vice President, Regulatory Affairs
and Chief Regulatory Counsel

Cardinal Health
7000 Cardinal Place
Dublin, OH 43017
614.757.7721 tel
614.652.4403 fax
robert.giacalone@cardinalhealth.com

www.cardinal.com

CardinalHealth

September 7, 2010

VIA Facsimile and U.S. Mail:

Attorney General Michael A. Delaney
New Hampshire State Attorney General's Office
33 Capitol Street
Concord, NH 03301

RE: Business Reporting a Breach of Security

Dear Attorney General Delaney:

Pursuant to applicable state law, we write to notify you of a data security event at the Dublin, Ohio facility of Cardinal Health (the "Company"). To date, the incident involves the potential unauthorized access to certain personal information of approximately 4 residents of your state.

Description of the Security Event

In mid-June, 2010, a third party notified us that he purchased a laptop on eBay that appeared to have originated from our Company. We recovered that laptop and conducted an investigation. We determined that the laptop did not contain any personal information. We also learned that the laptop recently had been decommissioned from use and replaced with a new one. Company policy requires that when a computer is decommissioned, the responsible IT employee must erase its data and then arrange for its destruction through our approved vendor. During our investigation, an IT employee admitted that, rather than arrange for its destruction, he took the laptop in question and sold it on eBay. The IT employee denies taking or selling any other Company computers. We have since terminated his employment. Based on this incident, we re-inventoried our computers, including all decommissioned computers. This process revealed by the end of July, 2010, that we could not account for nine (9) laptops and two (2) desktops that had been decommissioned and slated for erasure and destruction. Because these computers had all been replaced, the Company retained a complete copy of the data on these missing computers. The Company analyzed the data from the missing computers and in late August, 2010, concluded that one of the laptops had been used by an HR employee and contained personal information that included employee number, birth date and social security number for current and former Company employees, as well as birth dates and social security numbers for some job applicants.

Steps the Company is Taking to Protect the Affected Persons

At this point, we can only confirm that these computers are missing. We have no information that the computers have been taken from Company premises or otherwise accessed without authorization, and we hope to still locate the missing computers during our further search efforts. Out of an abundance of caution, however, and given that the IT employee admitted to selling one decommissioned computer on eBay, we have elected to notify the employees and applicants whose personal information was on the one missing HR laptop. A sample copy of that notice is enclosed and it will be distributed to affected persons on or about the same date as this letter. The notice explains how to place a fraud alert with the relevant credit reporting agencies, and provides appropriate telephone and e-mail contact information in the event the individual has questions regarding this process or the underlying incident. Finally, the Company is offering to all affected persons a credit monitoring service from a very reputable vendor for a period of one full year at no cost to the individual. This service includes assistance with addressing any fraudulent activity on personal accounts, as well as comprehensive identity theft insurance coverage and other important features.

In addition to providing these services to the affected individuals, we have reviewed our internal procedures concerning decommissioned computers and are making adjustments to address the risk of future theft and loss. For example, we have restricted access to inventory rooms where computers are stored, and we have installed a surveillance camera in a strategic location to monitor inventory room activity and to act as a deterrent. We also have revised and improved our decommissioned computer destruction policy, and have instituted mandatory training for all applicable IT employees to reinforce proper disposal practices.

We deeply regret that this incident occurred and we will work hard to quickly address and resolve any further issues. If you have any questions, please feel free to contact me directly. I can be reached at Monday through Friday. Thank you for your time and attention to this matter.

Yours very truly,

Robert P. Giacalone, R.Ph., J.D.*

* Licensed to practice law and pharmacy in Ohio and Illinois.

[Date]

EE name
EE address 1
EE address 2

Dear EE name

This letter is to notify you of a potential security breach at the Dublin, Ohio facility of Cardinal Health (the "Company") involving potentially unauthorized access to your personal information.

In mid-June, 2010, a third party notified the Company that he purchased a laptop on eBay that appeared to have originated from our Company. We recovered that laptop and conducted an investigation. We determined that the laptop did not contain any personal information.

Based on this incident, we re-inventoried our computers. This process revealed by the end of July, 2010, that we could not account for nine (9) laptops and two (2) desktops that had been decommissioned and replaced. Because these computers had all been replaced, the Company retained a complete copy of the data on these missing computers. The Company analyzed the data and in late August, 2010, concluded that one of the laptops contained personal information that included employee number, birth date and social security number for current and former Company employees, as well as birth dates and social security numbers for some job applicants. At this point, we can only confirm that these computers are missing. We have no information that the computers have been taken from Company premises or otherwise accessed without authorization, and we hope to still locate the missing computers during our further search efforts. While the Company believes that there is low risk that your personal information will be used inappropriately, we can understand that you might be concerned.

As a preventative measure, therefore, and to help strengthen the integrity of your personal information, we are providing you with certain information about how to protect yourself from identify theft. Please see **Attachment 1** for this information. In addition, out of an abundance of caution, we have arranged for you to have the option to receive 12 months of identity protection under the Debix Identity Protection Network **at no cost to you**. More information about this service is available on **Attachment 2**. When you set up your account following the enclosed instructions, Debix will enroll you in OnCall Credit Monitoring™ and you will receive OnCall Credit alerts regarding changes in your credit file over the next 12 months. Using your phone, you will be able to review and verify these credit alerts and Debix on-call investigators will be there to assist you in the event that you suspect fraud. This service also includes a $1,000,000 Identity Theft Insurance Policy, and 12 months enrollment in Debix Fraud Resolution Services, if needed, to assist you in restoring your credit file should that become necessary. Again, this service is optional and will be provided to you at no cost if you decide to use it.

Debix has a simple Internet-based verification and enrollment process. To sign up, go to http://www.debix.com/safe. You will need to provide the activation code that is listed at the top of this letter. Once you have entered your activation code, click on "Sign up now" on the right side of the webpage and follow the website's instructions. Please note that if you enroll online, part of the sign-up process may include receiving a phone call from Debix soon after you initiate the registration process.

If you do not want to enroll on-line, you can register with Debix over the telephone by calling 888-332-4963. If you prefer to register via the U.S. Postal Service, we have included a mail-in registration form.

You will have 90 days from receipt of this letter to register for the OnCall Credit Monitoring™. This service will be valid for one year from the date you register. If you have questions about Debix or its coverage, please contact them directly at 888-332-4963. Their support is available Monday through Friday, 9 a.m. to 5 p.m. Central time.

The security of your personal information is important to us, and we work hard to ensure we have processes in place to keep it safe. We deeply regret this situation and any inconvenience and concern it may cause you. If you have questions for the Company please email them to gmb-dub-Ethics&Compliance@cardinalhealth.com or contact the Cardinal Health Ethics and Compliance Department at 614-757-7504, Monday through Friday, 8:00 a.m. to 5:00 p.m. Eastern time, excluding holidays.

Sincerely,

Ed Daniels
Vice President, Ethics and Compliance
Cardinal Health

Attachment 1

Additional Information on Identity Theft Prevention

Even if you do not feel the need to register for the credit monitoring service, we recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (you can print a copy of the request form at http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm). You can also purchase a copy of your credit report by contacting one of the three national credit reporting companies:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790

When you receive your credit reports, review them carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to proper law enforcement authorities, including local law enforcement. You may contact the Federal Trade Commission ("FTC") or your local state Attorney General's Office, or the national credit reporting agencies listed above, to learn about preventing identity theft and to obtain additional information about avoiding identity theft.

For all U.S. Residents, you can contact:	Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) http://www.ftc.gov/idtheft/
In addition, North Carolina Residents can contact:	North Carolina Attorney General's Office Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 Telephone: 1-877-5-NO-SCAM http://ncdoj.gov/
In addition, Maryland Residents can contact:	Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. An initial fraud alert stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An extended fraud alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you have been a victim of identity theft and you provide the credit reporting company with the documentary proof it requires. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three credit reporting companies provided above.

Credit Freezes: You have the right to put a "credit freeze" on your credit file so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift, and/or remove a credit freeze. In addition, you may incur fees to place, lift, and/or remove a credit freeze. These fees generally range from $5-20 per action. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies at the numbers above to find out more information.

Attachment 2

Free identity protection. Priceless peace of mind.

ENROLL NOW! Free Identity Protection That's Proven to Work.

Debix provides a new level of identity protection no other company can match. Only Debix has an Identity Protection Network that identifies potential attacks and delivers critical information to you by phone.

What You Get:

- ID Theft insurance covers financial losses
- Comprehensive identity repair
- Early attack detection
- Live OnCall investigators assist you if an attack occurs
- Cancel and replace credit cards if your wallet is lost or stolen

Free, Fast, Simple Enrollment.

Insurance Amount: $1,000,000

ENROLL NOW
Activation Code: <<ActivationCode>>

Online: www.debix.com/safe

By Mail: Form included in letter

Phone: Toll-free 866-979-2595

Representatives available 9 AM – 5 PM Central Time, Monday through Saturday

Sign Up Today For Your FREE Identity Protection From Debix.

Debix Identity Protection. What's included?

OnCall Credit Monitoring. Debix constantly scans credit records for signs of financial, medical and criminal identity theft.	**OnCall Credit Alerts by Phone.** If there are changes to your credit file - like evidence that a thief has used your credit, you will get a secure call from Debix.	**OnCall Investigators.** If you suspect fraud, experienced and helpful specialists will repair your identity, saving you hundreds of hours of headache.	**Identity Theft Insurance.** If a thief steals your identity you will be reimbursed for covered financial losses.

www.debix.com/safe

DEBIX
The Identity Protection Network