



SECURING HIGHER EDUCATION

EHI INTEGRITY



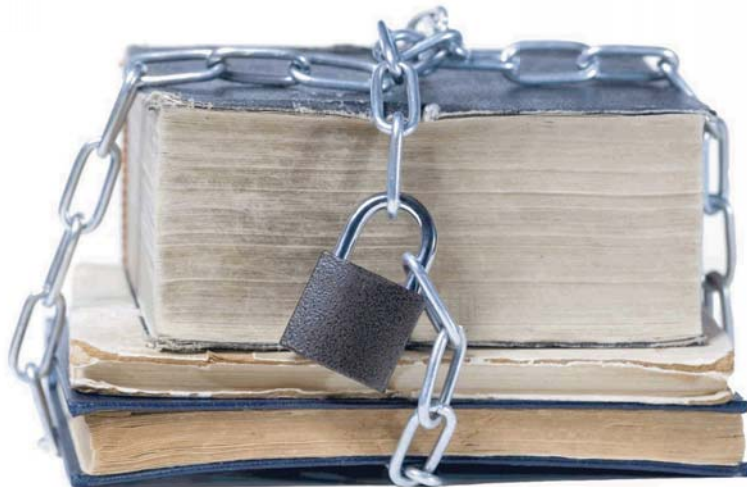
ATLANTA, GEORGIA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a law that charges the Department of Health and Human Services to establish regulations for the handling of certain types of health information (EHI), collectively known as "protected health information." HIPAA itself does not establish the regulations, but provides the framework for regulations (generally known as "rules")

» cont., **PG. 2**

IDENTITY FRAUD:

Don't become a part
of what's become
a \$45 billion dollar
problem.

PG 2



GAINESVILLE, FLORIDA - In mid February, a foreign hacker gained access to a University of Florida computer system containing the personal information of students, faculty and staff. The files included the names and Social Security numbers of individuals who used UF's Grove computer system since 1996. Number of records at risk? **97,200.**

Binghamton University in New York kept payment information for every student, possibly dating back at least 10 years in a storage area next to one of the most trafficked lecture halls on campus, behind a door that was not only unlocked but taped open.

The information itself contained Social Security numbers, credit card numbers, scans of tax forms, business information (including Social Security numbers and salary information for employees of students' parents), asylum records and more, all kept in a haphazard and disorganized fashion, sprawled out in boxes, in unlocked

(yet lockable) filing cabinets and shelving units.

If the information inside the room pertained only to the current students enrolled and their parents that would mean the story would affect, roughly, 42,000 people. However, because the information goes back at least 10 years, if not more, the potential number of people affect lies well in the hundred thousands. Number of records at risk in this scenario? **100,000.**

Technology; the Internet; virtual universities and classrooms anytime – anywhere (remote) access; high-speed, reliable, and strong network infrastructures all play an important and meaningful role in enabling higher education institutions to further the initiatives set forth by the executive management.

Today's enterprises have extensive electronic communication pathways (computer networks and telephone systems for example) extending well beyond the

» cont., **PG. 2**

PODCAST



Beginning in March, the USG Office of Information Security launched a series of podcasts covering a wide range of security-related topics. The first three podcasts in the series speak to the following topics:

- "Stan Gatewood's First 100 Days As Chief of Information Security"
- "What is Cyber-Security?"
- "Policy Standard Guidelines"

Visit <http://itunes.usg.edu/> for more information

physical bounds of their operations. Internal vulnerabilities may be exploited by external threats as well as internal.

It seems that everything relies on computers and the Internet these days — communications (email, texting, cell phones), entertainment (satellite, MP3s, podcasts), transportation (car navigation systems, airline ticketing), shopping (online stores, e-commerce, credit cards), medicine (equipment, medical records), and the list goes on. How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system?

Cyber security involves protecting that information by preventing, detecting, and responding to attacks.

There are many risks, some more serious than others. Among these dangers are viruses erasing your entire system, someone breaking into your system and altering files, someone using your computer to attack others, or someone stealing your credit card information and making unauthorized purchases.

Unfortunately, there's no 100% guarantee that even with the best precautions some of these things won't happen to you, but there are steps you can take to minimize the chances.

EHI INTEGRITY, continued

in four areas: transactions and code sets, identifiers, privacy, and security.

Each USG institution that inputs, processes, stores, or transmits electronic health information (EHI) must be concerned with the confidentiality, integrity, and availability of EHI. "Electronic health information" includes any identifiable health information relating to the health of an individual, the care provided or payment for care EHI includes information in any form or medium (electronic, paper, verbal, etc.)

Because HIPAA is technology neutral, USG healthcare organizations will be responsible for understanding how to maintain security in their proprietary network environment. It is imperative that the institutions understand that there is always a certain level of risk, and that they must always have a strategy for addressing them.



The Internet has also made it easier for thieves to sell or trade the information, making it more difficult for law enforcement to identify and apprehend the criminals.

- Stan Gatewood, CISO
University System of Georgia



This will require the institution to:

- *Have current data on their security products' strengths and limitations.*
- *Understand current exploit methods.*
- *Deploy measurable security criteria to ensure that the technology remains secure over time.*

HIPAA does not set rigid, specific requirements, but rests the burden of applied, appropriate action on the institution.

For more information, visit:

[HTTP://WWW.HHS.GOV/OCR/PRIVACY/INDEX.HTML](http://www.hhs.gov/ocr/privacy/index.html)

TO CATCH AN IDENTITY THIEF

IDENTITY THEFT is the taking of someone's personal information and using it for an unlawful purpose. It is a serious crime with serious consequences. Identity theft, or identity fraud, is a crime that can have substantial financial and emotional consequences. Take precautions with personal information; and if you become a victim, act immediately to minimize the damage.

There were 8.1 million U.S. residents who were victims of identity theft in 2007. That represents 3.6% of adults, including thousands of Georgians. The total cost of identity theft in 2007 was \$45 billion.

According to the Federal Trade Commission's 2007 report, 59% of identity theft involves existing credit card accounts. Forty-nine percent involves other existing accounts, such as bank accounts and utilities. And 22% involves new accounts and other non-account-related forms of the crime. (Note: the numbers add up to more than 100% because some cases involve more than one form of identity theft.) It is the third type, new account and non-account identity theft, that can be the most difficult to resolve. Such victims may spend hundreds of hours and thousands of dollars clearing up their records and their lives.

You can be a victim of identity theft even if you never use a computer. Malicious people may be able to obtain personal information (such as credit card numbers, phone numbers, account numbers, and addresses) by stealing your wallet, overhearing a phone conversation, rummaging through your trash (a practice known as dumpster diving), or picking up a receipt at a restaurant that has your account number on it. If a thief has enough information, he or she may be able to impersonate you to purchase items, open new accounts, or apply for loans.

The Internet has made it easier for thieves to obtain personal and financial data. Being aware of how information is illicitly obtained and misused is the first step to **not** being a victim.

MORE INFORMATION...

USG Office of Information Security
706-583-2001 or 888-875-3697

www.usg.edu/infosec

