News

Published on Friday, January 21, 2005

Drug Records, Confidential Data Vulnerable

Harvard ID numbers, PharmaCare loophole provide wide-ranging access to private data

By J. HALE RUSSELL and ELISABETH S. THEODORE

Crimson Staff Writers

The confidential drug purchase histories of many Harvard students and employees have been available for months to any internet user, as have the e-mail addresses of high-profile undergraduates whose contact information the University legally must conceal, a Crimson investigation has found.

Administrators shut down a Harvard website contributing to the breach minutes after The Crimson demonstrated the problem yesterday afternoon. But at press time, sensitive data—including the drug histories of those insured by the University—remained vulnerable to anyone who obtains a student or professor's non-confidential Harvard ID number.

The now-disabled Harvard website, iCommons Poll Tool, required nothing more than a free, anonymous Hotmail account and five minutes to look up the eight-digit ID of any student, faculty or staff member.

THE CRIMSON STAFF

FROM STEPHEN TO ZITHROMAX (STEP 1/3, next for more) Starting with nothing more than a consenting undergraduate's first name, The Crimson generated, in 10 minutes, a list of all prescription drugs he had ever purchased at University Health Services Pharmacy.

Total Pictures: 3 >

Article Options

- Email this article to a friend
- Send a letter to the editor
- Print this article

A list of all three prescription drugs purchased by one student at University Health Services (UHS) Pharmacy was accessed by The Crimson by typing his ID number and birthday into another website, run by Harvard drug insurer PharmaCare. Birthdates of undergraduates are published to fellow students, and are in many cases more widely available on sites such as anybirthday.com.

Last night, the insurer's website still required nothing more than these two pieces of information to provide a list of drugs purchased by anyone covered by Harvard's drug insurance policy—which is mandatory for all undergraduates and also covers many faculty and staff.

UHS, after being alerted to the security issues on PharmaCare's website by The Crimson yesterday, said it immediately called the insurer for an explanation.

"We're in contact with PharmaCare," UHS Compliance Officer Barbara Skane

said yesterday evening. “We’ve expressed to them how serious this is and that we’re asking their senior management to look into it to see what we can do to correct any inappropriate access.” She added she did not yet know whether PharmaCare’s website might violate HIPAA, a federal law prohibiting the unauthorized disclosure of individual medical records.

Moreover, from the now-disabled University website, it took under a minute to produce the ID number and e-mail address of a student who told The Crimson he had been granted security status at Harvard under the Family Educational Rights and Privacy Act (FERPA) because his family is prominent in international politics.

“If a student contacts their Registrar and requests total privacy under FERPA, this FERPA status...must also [be] recorded in the central directory system,” wrote Jane E. Hill, Harvard’s Directory Services project manager, in an e-mail.

FERPA legally requires universities not to disclose or verify directory information, including names and e-mail addresses, of individuals with a secure flag, except as required for specific educational purposes. This protection is used both by “publicity-shy” celebrities and for students who “are legitimately terrified of some potentially harmful person—a woman trying to disappear from a stalker, for example,” wrote former Dean of the College Harry R. Lewis ’68 in an e-mail.

Additionally, though Faculty policy prohibits it, many professors still e-mail their students all class grades listed by ID numbers. Thus any of the 311 students in Psychology 1 this year, among others, could have also used the disabled website to determine what exam grades their classmates received—a confidential academic record.

After the iCommons Poll Tool was shut down last night, University Technology Security Officer Scott Bradner said that “there’s no condition under which [the ID number] should have been shared…It was not a design feature.”

The glitch—and the vulnerabilities that remain—underscore the difficulties posed to information privacy by the widespread use of ID numbers to verify identity, even though those numbers are often not kept secret.

“The University has a custodial obligation to protect the personal information of its students, its faculty and its employees,” said Marc Rotenberg ’82, executive director of the Electronic Privacy Information Center, after learning of The Crimson’s findings. “People need to understand how pervasive the University’s information gathering and collating capabilities are…The impact on the Harvard community in terms of the privacy exposure is substantial.”

SKELETON KEYS

These vulnerabilities stem from Harvard’s use of a non-confidential number to verify identity and access secure systems. ID numbers, which Bradner says are considered “non-public but not secret,” are often widely distributed—to course heads and staff, on printed ID cards and even to students planning a barbecue.

Though most Harvard websites with secure information require a confidential PIN or other password in addition to the ID, The Crimson has identified a number of online applications—ranging from PharmaCare to network access to mail forwarding—that require nothing more than an ID

number and birthday, or ID and last name.

Computer security experts say such use of a non-secure identifier as a password is a serious and common problem.

“The ID number, much like the Social Security Number, has always had this problem of operating both as a record identifier and as a password,” Rotenberg said. “It’s the interchangeable nature of the identifier that creates a security risk.”

Until yesterday afternoon, exploiting such vulnerabilities could have been made easier by the long-standing glitch in the polling tool. The website, which allows people to design and conduct surveys, enabled anyone—with or without Harvard affiliation—to search the entire Harvard directory by first or last name, e-mail address or Harvard ID number. Unlike other campus directories, the system did not hide users who have requested FERPA security from the University, or respect other user-set restrictions on the distribution of their directory data.

A series of steps common in conducting a poll enabled any iCommons user to directly look up the ID number of any Harvard affiliate—from secure-flagged students to University President Lawrence H. Summers. No other public system permits students to search ID numbers or to associate ID numbers with names.

Susan Rogers, project manager for iCommons, was surprised when The Crimson demonstrated the technique for looking up a FERPA protected student’s information, though she had previously planned to remove the search by ID number feature.

She added yesterday evening that preliminary analysis of the usage logs of the poll tool showed that prior to pulling the site, only The Crimson had used the method that non-Harvard affiliates could use to gain access.

BEHIND UNPINNED DOORS

But even if iCommons is fixed, The Crimson has identified a variety of web tools that require no more than the non-secret ID, or a combination of ID and last name or birthday, to access information that would generally be considered confidential.

For instance, anyone on campus can delete or register a Harvard network connection just knowing an individual’s ID and last name. This would permit someone to illegally share files traceable to another person’s identity.

A last name and ID are also the keys to choosing course sections and accessing the Student Employment Office’s jobs database. Only an ID is required to access the Office of Career Services’ MonsterTrak job listings database.

With a Harvard ID and birthday—obtainable by undergraduates through an online facebook, and more widely through websites like anybirthday.com—a user can post or download resumés on someone else’s eRecruiting account or access the online UHS health insurance waiver form. Individuals can also activate an e-mail address for someone who is eligible for a Faculty of Arts and Sciences account but has not requested one.

Setting up all campus mail to forward to a different physical address requires the ID and the last four digits of a student’s social security number —often obtainable by searching online directories like Lexis-Nexis and

Accurint. Accessing mail forwarding would also show the individual's current Harvard address, which for a secure-flag student could result in the disclosure of their on-campus whereabouts.

The most sensitive data accessible with only a Harvard ID and birthday, though, appears to be that from Harvard's primary drug insurance provider, PharmaCare.

Bradner said the healthcare industry is under unusually strict requirements to protect sensitive information, in part due to HIPAA.

"Despite that, there are a lot of people in the healthcare industry who just don't get it," he said. "If indeed they're using just [ID and birthday] to identify somebody, that's an example of just not getting it."

Skane, the UHS compliance officer, said that without more information from PharmaCare she was unsure whether Harvard or PharmaCare would be able to determine whether unauthorized individuals had used the site.

A PharmaCare spokeswoman last night said she was unaware that information about past pharmacy drug purchases was available through its website.

Jerome B. Tichner Jr., an attorney practicing healthcare law at Boston-based Brown and Rudnick, said that while he could not comment on PharmaCare's specific case, current law requires insurance providers to "maintain reasonable safeguards to protect against improper access and disclosure of healthcare records."

"If an entity [covered by HIPAA] does not have adequate security systems, and it's very easy for any third party to walk in or log in and obtain pharmaceutical information or other…healthcare information, that may pose liability concerns," he said.

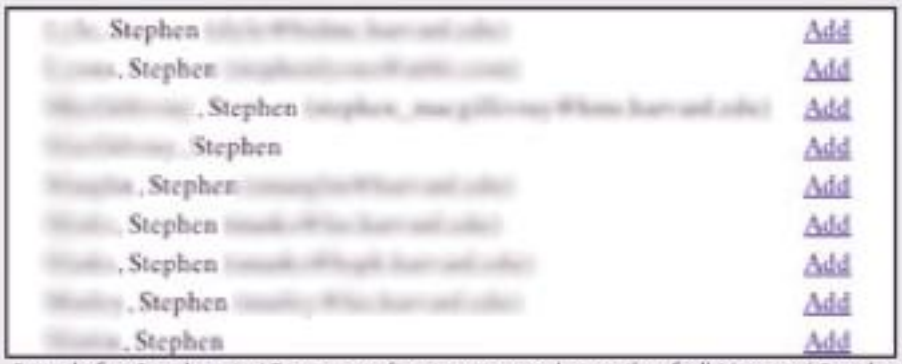
Lewis, who is also a computer science professor and will teach a Core course next semester on computers and public policy, said he has advocated since 1996 for clearer Harvard policies on ID privacy.

"Ten years ago the most you could get with a Harvard ID number was a bag lunch," he said. "But now data of all kinds are on web servers for reasons of convenience, and those Harvard ID numbers, if those are the keys, suddenly are much more powerful tools to get at sensitive information."

"It's too bad that everything hasn't been shifted over to PIN authentication, which should today represent the minimum of security for confidential university records," Lewis added.

—Staff writer J. Hale Russell can be reached at jrussell@fas.harvard.edu.

—Staff writer Elisabeth S. Theodore can be reached at theodore@fas.harvard.edu.



Search for Stephen in iCommons lists names and e-mails of all Harvard Stephens.

12	Total number of responses to the poll: 1		
13			
14	GROUP: testing		
15	Total number of group members: 5		
16	Number of group members who have responded to the poll: 1		
17	The following group members have not responded to this poll:		
18	NAME	HARVARD ID	EMAIL
19	Benedict Gross	802[redacted]0	gross@math.harvard.edu
20	Steven Hyman	701[redacted]6	steven_hyman@harvard.edu
21	William Kirby	503[redacted]1	william_kirby@harvard.edu
22	Lawrence Summers	200[redacted]3	lawrence_summers@harvard.edu
23			
24			
25			
26			

pollNonRespondents-2

Sample results generated by iCommons displaying Harvard ID numbers.