WHITE PAPER

Healthcare Kiosks Can Improve Efficiency and Protect Patient Identities as Red Flag Rules Take Effect

Medical identity theft is a growing problem, and new federal laws are putting the burden of keeping patient information safe on healthcare providers. Self-service kiosks in hospitals and medical practices can help providers increase efficiency and comply with regulations.

Developed and published by:

KioskMarketplace
KIOSK NEWS, TRENDS & COMMENTARY

Sponsored by:

UCoA
UNICOMP CORP. OF AMERICA

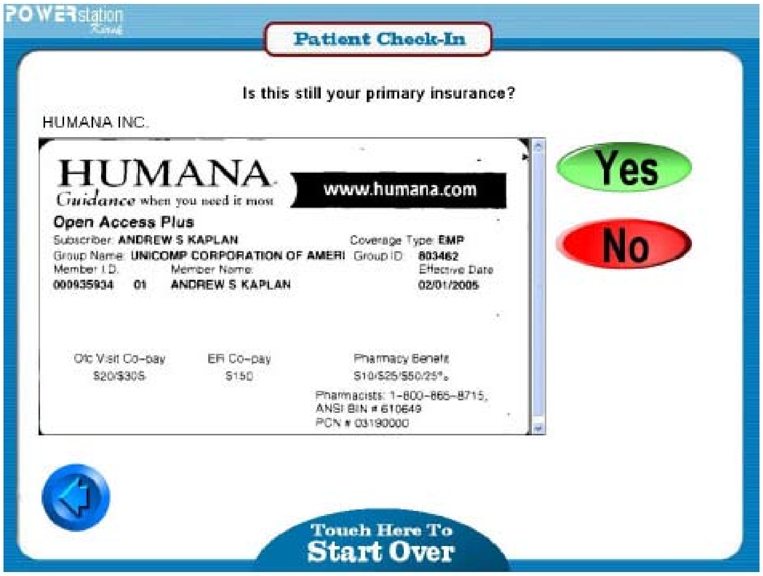
By Darcy Lewis
Contributing writer,
KioskMarketplace.com

In recent years, self-service kiosks have shown themselves to be valuable additions to the healthcare environment. When used to check in patients, kiosks increase staff efficiency and decrease patient waiting times by automating routine registration procedures and decreasing paperwork. But now technologically savvy hospitals and clinical practices realize that kiosks also present a defense against the growing threat of medical identity theft.

Kiosks are ideally suited for tasks like automatically confirming that a given patient has an appointment with a specific physician at a specific time, freeing up a staff member from having to do that manually. And consider the old registration process of having a clerk make photocopies of the patient's insurance card and driver's license, verify insurance coverage and present multiple forms for the patient to sign.

Today's kiosks enable the patient to perform these types of tasks for himself quickly and easily using software that keeps personal information secure, while HIPAA-compliant screens shield the user's data from view.

For example, the kiosk allows the patient to verify that his insurance coverage is unchanged from a previous visit. Do new or updated forms need to be signed? No problem, since they can be signed electronically at the kiosk and then stored as part of the patient's chart.



Is this still your primary insurance?

HUMANA INC.

HUMANA
Guidance when you need it most
www.humana.com
Open Access Plus
Subscriber: ANDREW S KAPLAN   Coverage Type: EMP
Group Name: UNICOMP CORPORATION OF AMERI   Group ID: 803462
Member I.D.   Member Name: Effective Date
000935934 01   ANDREW S KAPLAN   02/01/2005

Ofc Visit Co-pay: $20/$30S
ER Co-pay: $150
Pharmacy Benefit: $10/$25/$50/25%
Pharmacists: 1-800-865-8715,
ANSI BIN # 610649
PCN # 03190000

Self-service kiosks can perform tasks like verifying patient insurance has stayed the same, freeing staff to do other tasks.

By performing real-time insurance benefits and eligibility verification, kiosks can even tell the patient what his deductible and co-pay are for the visit and collect payment for that and any outstanding balance, all before the patient sets foot in an examination room.

Scope of the crime

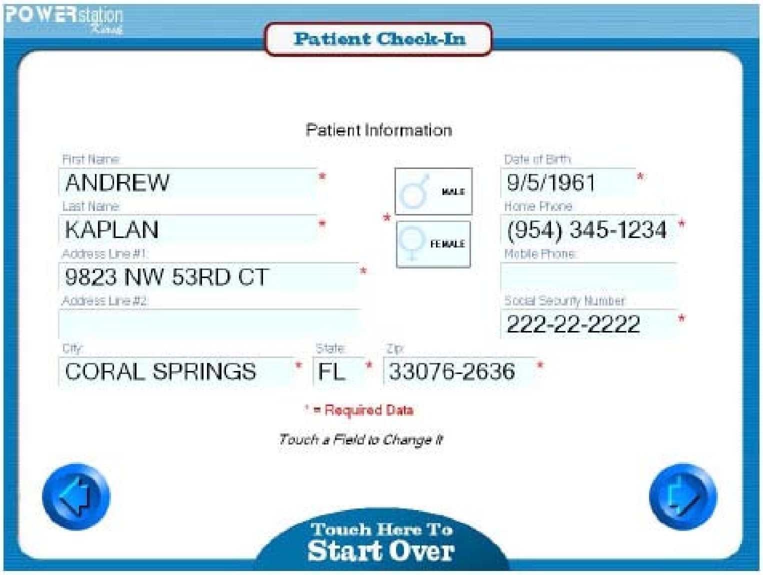
The medical identity theft problem is large growing, while solutions have been elusive. Medical identity theft is a troublesome blend of healthcare fraud and identity theft combined into a toxic stew that has skyrocketed in recent years, significantly affecting providers, insurers and patients. There is a simple reason: Until now, medical identity theft has been difficult to detect.

© 2009 NetWorld Alliance LLC

There are two main types of medical identity theft, according to Government Technology. One type involves physician identification numbers being stolen and used to bill for services. The second type occurs when patient identification information is stolen and used to obtain services or to bill for services fraudulently.

The World Privacy Forum conducted the first study on medical identity theft in 2006. It found that the crime accounts for 2.7 to 3.2 percent of total identity theft, widely characterized as the fastest-growing crime of the 21st century.

In 2008, the Federal Trade Commission (FTC) estimated that medical identity theft comprised 3 percent of all identity theft cases in the United States, or 300,000 cases per year. And it's reasonable to assume that the true numbers may be quite a bit higher, since many cases undoubtedly go undetected. In fact, Gartner Research estimates that there will be more than 1 million cases of medical identity theft in 2009. Altogether, individuals and businesses suffer billions of dollars in losses each year from medical identity theft, both in direct losses and in administrative and legal costs associated with investigating and resolving potentially fraudulent claims.



Patient Information

First Name: ANDREW *
Last Name: KAPLAN *
Address Line #1: 9823 NW 53RD CT *
Address Line #2:
City: CORAL SPRINGS * State: FL * Zip: 33076-2636 *
Date of Birth: 9/5/1961 *
Home Phone: (954) 345-1234 *
Mobile Phone:
Social Security Number: 222-22-2222 *

* = Required Data

Touch a Field to Change It

Identification screens can help ensure that the correct patient is checking in for the right appointment.

Red Flag Rules

At that same time, the FTC also published final guidelines in the Federal Register for reducing identity theft. The so-called Red Flag Rules require each financial institution or creditor that holds any consumer account to develop and implement a written Identity Theft Prevention Program for combating identity theft in connection with new and existing accounts (see: www.ftc.gov).

There was initial uncertainty about whether the rules applied to healthcare organizations. The FTC decided that healthcare providers who accept insurance, or bill the patient for services rendered, are considered to be creditors since they are deferring payment, i.e., extending credit to their patients.

After several postponements, the mandatory compliance date for all covered healthcare organizations, even small practices, was set for

August 1, 2009. Failure to comply could cost a healthcare organization up to $2,500 per violation.

According to the Red Flag Rules, the written program must include reasonable policies and procedures that enable the creditor to:

1. **Identify** relevant patterns, practices and specific forms of activity that are "red flags," signaling possible identity theft and incorporate them into the program;
2. **Detect** red flags that have been incorporated into the program;
3. **Respond** appropriately to any red flags detected; and
4. **Ensure** that the program is updated periodically to reflect changes in risk.

Healthcare practices have extensive leeway in how they implement the Red Flag Rules, says Andy Kaplan, president of Unicomp Corporation of America, a Coral Springs, Fla.-based provider of process automation products focusing on the business side of medicine.

> **"[Red Flag Rules] provide guidance for authenticating a patient's personal identifying information against external information sources."**
>
> **— Andy Kaplan, president, Unicomp Corporation of America**

"The Red Flag Rules don't specify any required procedures for detecting, preventing or mitigating identity theft," he said. "But they do provide guidance for authenticating a patient's personal identifying information against external information sources."

How kiosks help with Red Flag compliance

Accordingly, Unicomp sees the self-service kiosk as filling an important role in Red Flag Rules compliance because of their easy information gathering capability.

For example, during the patient registration process, a kiosk can automatically confirm personal data.

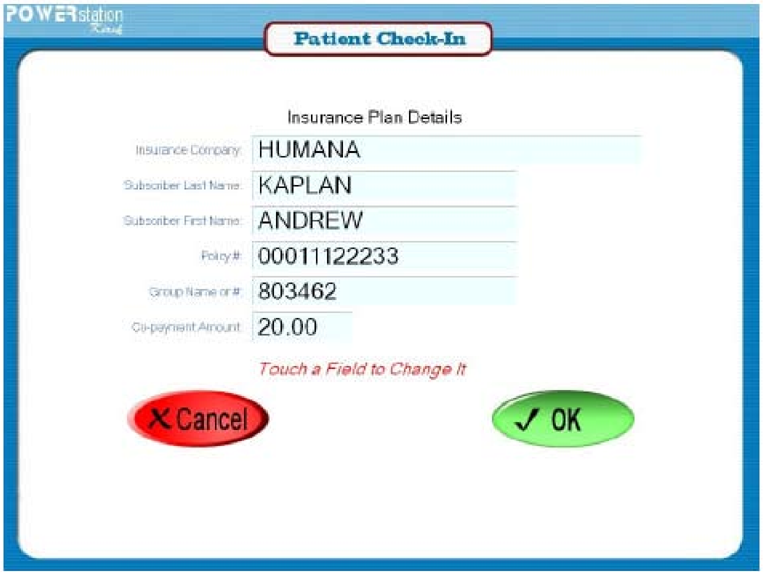
"Our POWERstation kiosk application provides real-time authentication of patient-supplied information by using the United States Postal Service, Social Security Administration and other public databases," said Kaplan.

If the kiosk notes a discrepancy, it politely prompts the patient to visit an available registrar, who can then investigate and handle the matter with the patient in the manner outlined in their Red Flag Rules written policy and procedures.

State-of-the art kiosks, like Unicomp's POWERstation, can allow patients to update their information, not just verify it. Once any data elements are edited, they need to be authenticated. This allows the software to pinpoint any discrepancy with major databases and flag the result. Then, the registrar determines whether the discrepancy has a plausible explanation or rises to the level of a red flag.

"Ultimately, as much as kiosks increase efficiency and reduce the potential for identity theft, the decision about whether there was truly an identity breach or not needs to be made by a human," said Kaplan. "But by the time the registrar gets involved, the kiosk will have done much of the preliminary work."

These uniquely versatile features lead Kaplan to believe that kiosks provide a helpful means for healthcare organizations to comply with the Red Flag Rules legislation.



Insurance Plan Details

Insurance Company:	HUMANA
Subscriber Last Name:	KAPLAN
Subscriber First Name:	ANDREW
Policy #:	00011122233
Group Name or #:	803462
Co-payment Amount:	20.00

Touch a Field to Change It

Kiosks can help confirm that a patient's information is correct, keeping a practice in compliance with Red Flag Rules.

"We know this is going to affect everyone in healthcare and we also know there is a lot of confusion about how best to comply," he said. "Having a kiosk won't give you all the answers, but it will help you comply with your written Red Flags program."

***About the sponsor:** Since 1979, Unicomp has specialized in developing cutting-edge document management and productivity solutions for the healthcare industry. Its IMPOWER products are used by over 20,000 physicians in more than 35 states. Unicomp has been delivering applications to help the patient registration process for more than eight years, as an integral part of the IMPOWER product suite.*

© 2009 NetWorld Alliance LLC