



and many other functions. But even within the border of our nation, we have all heard or read of stories about stolen government laptops, and lost backup tapes.

Last year CVS, the pharmacy giant, was fined \$2.25 million for failing to protect sensitive financial and medical information of its customers and employees.

More recently, 12,000 Medicare enrollees had their protected health information compromised by a simple filing cabinet donation gone wrong. Blue Cross & Blue Shield of Rhode Island donated a filing cabinet to a non-profit organization without first removing surveys that contained Medicare PHI (Protected Health Information).

While all these stories are awful, I believe the real danger still lies with individuals who work for doctors, clinics and hospitals. It is becoming alarmingly more common for clerical staff to steal patient records by downloading information on a flash drive and sell it on a black market, which can happen in a mere moment. This could be an unhappy employee or someone recently hired to take a position simply to purloin information.

Medical administrative staffs who commit medical identity theft are sophisticated professionals who are adept at making sure victims do not detect their crime. Victims may only discover it many years later through an unhappy circumstance such as the discovery of an incorrect blood type on a medical chart, or the loss of a job opportunity after a background check reveals one or more diagnoses and diseases that didn't belong to them.

Medical identity theft victims do not have an easy way to discover who, if anyone, to call for help. Because of how this crime is committed, in some situations, the same people victims may call for help may be among those perpetrating the crime.

A physician can be the victim of identity theft in his professional capacity. This type of identity theft is often the starting point for disseminating incorrect information about patients, and it is often seen when professional crime rings are involved. Thieves steal a physician's name, license number, forge a signature, falsify patient records, and forge prescriptions.

As the health care system transitions from paper-based to electronic record keeping, this crime will become easier to commit. Victims will find it more difficult to recover from medical identity theft as falsified medical records are disseminated and re-disseminated through computer networks.

Electronic medical records on the nationwide level will have to be assessed for medical identity theft. Given the insider nature of this crime, any digitization of medical files in electronic health records needs to be built with an understanding that some doctors, nurses, clinics, and hospitals, as well as their administrative staffs, may be thieves themselves. This poses significant security problems, but if these issues are not taken into account now, then electronic systems can become a means to potentially enable medical errors across the county and facilitate widespread medical identity theft.

Currently, the thought is that digitization of patient records will improve health care, reduce fraud, reduce medical errors, and save lives. But this does not account for the challenging reality of medical identity theft and the substantial problems it can introduce into such a system.

The Federal Trade Commission (FTC), which has studied financial identity theft, is not responsible for addressing medical issues. Medical identity theft falls to the Department of Health and Human Services (HHS), which has not focused on medical identity crimes. The Office of Inspector General (OIG) investigates cases of generalized health care fraud and abuse, which is concentrated on financial damage to the Medicare program.

The Fair Credit Reporting Act allows for recourse for victims of financial identity theft. In the medical arena the Health Information Portability and Accountability Act (HIPAA) allows free information exchange between the provider and insurance communities. Patients have to give up most of their rights in exchange for insurance payment.

The Office of Civil Rights at the Department of Health and Human Services should review the HIPAA privacy rule and propose changes to expand the rights of medical identity theft victims, allowing them to amend health records in a much easier way.

One of the most effective means of proactively discovering improper use of personal information is to review all claims paid by the insurance company for each family member. Health insurers should send each beneficiary a free annual listing of all claims that were paid and to whom. This option is available on their secure website. Unfortunately, the information can be incomplete.

## About The Author



Health Benefit Advocate (HBA) is a nationwide Health Claims Assistance company that offers personal medical claims advocacy services for your Employees. We serve as an extension of your Human Resource Department, taking over the function of complex healthcare claims resolution while maintaining HIPAA compliance.

Navigating the healthcare system is fraught with obstacles and complexities that require the time and skill of caring and experienced professionals. The HBA management team brings over sixty years of combined experience of understanding the mechanics of healthcare claims delivery and reimbursement. Hospital and Physician Billing, Coding, Nursing and Managed Care and Insurance Experts combine the essentials needed to decrypt and resolve medical claims issues on behalf of the employee.

If you would like more information on how HBA might be able to assist you in maximizing your employee benefits portfolio, please contact Katalin at 866-497-7892 x2 or email her at [katalin@healthbenefitadvocate.com](mailto:katalin@healthbenefitadvocate.com)