



GEORGETOWN UNIVERSITY

Institute for Health Care Research and Policy

**Testimony before the**  
**U.S. House of Representatives**  
**Committee on Financial Services**  
**Subcommittee on Financial Institutions and Consumer Credit**

**on**

**The Role of the Fair Credit Reporting Act in**  
**Employee Background Checks and the Collection of Medical Information**

**Joy L. Pritts, J.D.**  
**Assistant Research Professor**  
**Health Policy Institute, Georgetown University**

**June 17, 2003**

2233 Wisconsin Avenue, NW Suite 525 Washington, D.C. 20007  
(202) 687-0880 Fax: (202) 687-3110 *facsimile*  
[www.georgetown.edu/research/ihrp](http://www.georgetown.edu/research/ihrp)

## **I. INTRODUCTION**

Mr. Chairman and Members of the Subcommittee on Financial Institutions and Consumer Credit: Thank you for the opportunity to testify before you today on the role of the Fair Credit Reporting Act (FCRA) and the collection of medical information.

My name is Joy Pritts. I am an assistant research professor at Georgetown University's Health Policy Institute. My work at Georgetown focuses on state and federal laws that protect the privacy of medical information and how these laws interact.

Today, a vast array of organizations and persons can collect and use medical information. They range from health care providers to insurers to banks to employers. There is no one federal law that protects the privacy of health information in the hands of these various stakeholders. In spite of repeated Congressional efforts, the use and disclosure of medical information continues to be governed by a patchwork of legislation and regulations that apply different standards to different sectors of the marketplace.

The Fair Credit Reporting Act (FCRA) is but one piece of this patchwork. I have been asked to testify today on the Fair Credit Reporting Act, how it governs the collection of medical information and how it interacts with the privacy provisions of two other major federal laws: The Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act.

In order to put these laws in perspective, I will first address how health care consumers believe their medical information should be treated.

## **II. PUBLIC NEED AND DEMAND FOR CONFIDENTIAL TREATMENT OF MEDICAL INFORMATION**

The American public is very concerned about the confidentiality of their medical information. In a poll conducted by the Gallup Organization in 2000, 79 % of adults reported that it is very important to keep their medical records confidential. People are afraid that their medical records will fall into the wrong hands, leading to discrimination, loss of employment, loss of benefits, and unwanted exposure.

Consumers are particularly concerned about banks and insurance companies having access to their medical information. The 2000 Gallup survey reported that an overwhelming 95% of those polled opposed allowing banks to see their medical records without their permission. Similarly, 82% opposed allowing insurance companies to see their medical records without their authorization.

In many cases, consumers have acted on these concerns. A 1999 survey by Princeton Research Associates for the California HealthCare Foundation found that one out of every six adults engages in some sort of privacy protective behavior to keep their medical information confidential. These consumers pay out of pocket for care that is covered by insurance, doctor-hop, provide inaccurate information, and avoid care altogether to protect themselves against their health information falling into the wrong hands. We can only imagine how these numbers would increase if health care consumers were fully aware of how their medical information could be

shared among various organizations. The privacy protective behavior that results from these concerns is bad both for the individual health care consumer and for public health. It can result in the inadequate care or undetected and untreated health conditions for the individual consumer. It can also result in inaccurate and incomplete patient data, which compromises the integrity of health research and public health initiatives. Thus, failing to adequately protect the confidentiality of health information can have widespread adverse consequences on both individual and public health.

Yet, the federal laws in effect today do just that. They fail to cover all of those who collect and maintain medical information and they fail to impose adequate standards on those entities that they do cover.

### **III. FCRA, GLBA AND HIPAA: A PATCHWORK OF PRIVACY PROTECTIONS**

Currently, the use and disclosure of medical information is governed by a patchwork of federal legislation and regulations. My testimony today will focus on the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), how they govern the sharing of medical information among affiliates and how these acts interact.

Three central issues evolve when these laws are reviewed. First, these laws do not adequately protect the privacy of medical information. Second, it is unclear to what extent states can remedy these gaps. Third, it is unclear which federal law prevails when their standards conflict.

#### Fair Credit Reporting Act

The FCRA does not adequately protect much medical information collected by banks, insurers, and other financial institutions. FCRA primarily restricts the use and dissemination of credit reports by banks and other financial institutions. A vast quantity of information escapes these restrictions, however, because it falls outside of the definition of “credit report.” Financial institutions are free to distribute *without limitation* information about their own transactions and experiences with consumers. This transaction and experience information can, and often does, include medical information.

Many financial institutions collect medical information in the course of conducting their business. For example, life insurers collect medical information in the application process. Property and casualty insurers may collect vast amounts of health information in the course of their claims process. Banks may collect health information in the course of selling annuities or credit insurance. Banks that issue credit cards may have the additional capacity to data mine credit card information, which can contain information on payments for health care services. Under FCRA, this transaction and experience information, which includes medical information, can be shared freely among affiliates without any permission from the consumer.

Affiliates also may share financial information (other than transaction and experience information) so long as they give the consumer notice and the opportunity to opt out. This

regulatory scheme is based on two erroneous assumptions: That the notices provided will actually be readable by the general public; and that most consumers would give their permission if asked. An opt-out essentially presumes permission unless the consumer takes some affirmative action. The notices provided by financial institutions, however, are largely written in legalese and are incomprehensible to most consumers. Furthermore, polls have repeatedly shown that consumers want to be asked *before* their health information is shared with others.

The irony of the situation is hard to ignore. The vast majority of Americans oppose allowing banks and insurers to see their medical information without their permission. Yet the law permits this very activity.

The increase in the consolidation of the financial services market combined with the advances in technological capacity only threatens to exacerbate these threats to privacy.

FCRA should be amended to afford greater protection to medical information. Consumers should be asked in advance, in plain language, whether they want their information shared in this fashion. Financial institutions should be prohibited from using medical information to provide credit.

The banking industry asserts that it does not use not medical information for making credit determinations. But an April 1993 U.S. Department of Health and Human Services task force report cited the case of a banker who also served on his county's health board. The banker apparently cross-referenced customer accounts with patient information and called due the mortgages of those suffering from cancer.

Furthermore, the fact that the banking industry does not engage in certain behavior now is no guarantee that it will not do so in the future. Fifteen years ago, it was virtually unheard of for insurers to use consumer credit histories to determine insurance premiums or whether to cancel or renew an insurance policy. Now, it is becoming increasingly commonplace. Who can say whether using medical information for credit decisions will develop along the same lines?

The time to prohibit such practices is *before* they become engrained as a standard business practice. As we have seen from the development of the Health Privacy Rules promulgated under HIPAA, once an information sharing practice becomes acceptable it is almost impossible to retract it.

A further concern with FCRA is the manner in which it potentially affects state law. Some states have taken steps to impose protections on the sharing of financial information that go beyond those provided by FCRA. It is unclear whether these state protections would survive a legal challenge. FCRA preempts states from enacting laws "with respect to the exchange of information among persons affiliated by common ownership or common corporate control." Some stakeholders interpret this provision narrowly and assert that FCRA only preempts state laws that govern consumer reports. Others, however, read this provision broadly and claim that it preempts states from enacting *any law* that governs the sharing of any information among affiliates. If this latter construction were accurate, a state would be prevented from requiring a

financial institution from obtaining consumers' permission (opt in) before sharing medical information with affiliates.

The simplest manner of resolving this ambiguity is to allow the preemption provision of FCRA to expire as scheduled on January 1, 2004. At a very minimum, FCRA should clarify that it does not preempt state laws that impose greater restrictions on the sharing of medical information.

The inadequacies of the FCRA have not been resolved with subsequent legislation. To the contrary, the Gramm-Leach-Bliley Act continues the pattern of allowing medical information to be shared freely among affiliated entities.

### Gramm-Leach Bliley Act and the Fair Credit Reporting Act

GLBA was enacted in 1999 to enhance competition by permitting the affiliation of banks, security firms, insurance companies, and other providers of financial services. The premise was to promote "one stop shopping" for financial services.

Recognizing that the creation of integrated financial services firms would exacerbate threats to consumers' privacy, Congress incorporated Title V into GLBA. Title V governs the privacy of personally identifiable financial information held by financial institutions. "Personally identifiable financial information" is defined broadly as including any information that is provided by a consumer to a financial institution to obtain a financial product or service or that a financial institution obtains about a consumer in connection with providing a financial product. Title V therefore governs any medical information that is provided to or obtained by a financial institution about an individual in connection with a financial service or product.

The "protection" afforded by Title V is *de minimus*. Title V permits affiliates to freely share medical information *without* any permission from the individual. As for disclosures to non-affiliates, Title V only requires notice of the potential disclosure and an opportunity to opt-out. There is *no* opt out provision for affiliates in GLBA. Neither is there a right to opt out of sharing with non-affiliated third parties when there is a joint marketing relationship between the financial institution and the other party.

As discussed above, many financial institutions such as life insurers, banks, and property and casualty insurers collect medical information in the course of conducting their business. Under GLBA these financial institutions can freely exchange this information. For example, under GLBA, a bank would be permitted to obtain and use medical information from a life insurer to determine eligibility or set the rate for a credit card or mortgage. This simply should not be permitted.

Congress provided the potential for some relief for consumers by including in GLBA a provision that essentially provides that Title will not preempt state laws that offer greater protection. A few states have moved in this direction.

It remains unclear, however, how far states can go in controlling the flow of consumer information among affiliates. The confusion stems from the presence in Title V of two provisions that address the preemption issue in what may be seen as a contrary fashion. Section 507 provides that Title V does not preempt state laws that offer greater privacy protections than GLBA. This provision would preserve a state law that requires an opt in for affiliates to share medical information.

Section 506 of GLBA, however, essentially preserves FCRA. As discussed above, FCRA not only allows the sharing of transaction and experience data without the consumer's authorization it also states from enacting laws "with respect to the exchange of information among persons affiliated by common ownership or common corporate control." The question remains: Can states enact legislation that restricts the sharing of consumer information among affiliates? Or are states limited to enacting legislation that only pertains to sharing information among non-affiliated entities? Rather than wait for court interpretation, Congress has a duty to clarify this issue.

As discussed below, the interpretation of FCRA and GLBA remains important due to the limited nature of HIPAA.

#### Health Insurance Portability and Accountability Act

The primary federal law governing the use and disclosure of medical information is the Health Privacy Rule promulgated under HIPAA by the United States Department of Health and Human Services.<sup>1</sup> While the HIPAA Privacy Rule is extensive, it is by no means comprehensive. Because of the limited authority delegated by Congress, the rule is applicable to only a core group of persons and organizations that hold health information. The HIPAA Privacy Rule directly applies *only* to:

- health care providers that transmit claims-type information electronically;
- health plans; and
- health care clearinghouses.

Thus, HIPAA does *not* apply to most of the entities covered by FCRA and GLBA. HIPAA does not apply to banks, or life insurers, or property and casualty insurers. There is some overlap in that all three laws do govern health plans.

Health plans are financial institutions that clearly possess great quantities of medical information, both from applications for insurance and from claims for payment. HIPAA restricts the manner in which a health plans can use and disclose this health information. These restrictions vary widely depending on the purpose of the use or disclosure and the recipient of the health information. Since this hearing is concerned with affiliate-sharing, I will focus on the issue whether, under HIPAA, a health plan could share health information with an affiliate in order for the affiliate to use the health information for its business purposes. For example, could a health plan share health claims information with an affiliated bank so that the bank could use the information in determining eligibility or setting rates for a loan?

---

<sup>1</sup> 45 C.F.R. Part 164.

In very general terms, HIPAA would require the health plan to obtain the individual's prior authorization to disclose health information for the business purposes of the affiliate. To continue with the previous example, under HIPAA a health plan could *not* share health claims data with an affiliated bank for the bank to use in determining eligibility or setting rates for loans unless the health plan obtained the individual's prior authorization. HIPAA uses what is essentially an "opt in" approach.

HIPAA's approach to this issue is clearly superior to that of FCRA and GLBA. It is important to remember, however, that HIPAA has a very limited applicability. For instance, HIPAA does not cover life insurers, automobile insurance carriers, workers' compensation carriers, banks, property and casualty insurers and employers. All of these entities can collect medical information in the regular course of their business but fall outside the scope of HIPAA. They are simply not subject to HIPAA's opt in requirements for affiliate sharing. While some of these entities are subject to FCRA and GLBA, both of these have less stringent standards for the sharing of medical information among affiliates.

The area where HIPAA, FCRA and GLBA overlap is also problematic due to the lack of Congressional direction as to which law prevails. Health insurers, for instance, are subject to FCRA, GLBA and HIPAA. The HIPAA Privacy Regulations prohibit behavior that would be permitted under GLBA and FCRA. Furthermore, state laws that may be preserved under HIPAA, which does not preempt state laws that do not conflict with or are more stringent than the federal health privacy standards, could potentially be preempted under FCRA. For example, a state insurance law that requires an opt in to sharing health information with affiliates would be preserved under HIPAA. Under the strictest reading of the FCRA preemption provision (which is incorporated by GLBA), such a state law potentially could be prohibited.

Congress has been silent with respect to how GLBA and FCRA interact with HIPAA. Applying traditional statutory construction rules to determine which statute prevails in this situation is problematic to say the least. Generally, later enacted, more specific statutes prevail. HIPAA was enacted in 1996. While the HIPAA regulations are very specific, the statute itself is fairly general with respect to the privacy of information. The amendments to FCRA permitting experience and transaction sharing among affiliates and preempting state laws were enacted in 1997 and are also fairly general. GLBA was enacted in 1999, after the HIPAA statute but before the HIPAA regulations were promulgated. The HIPAA regulations are extremely detailed. But comparing detailed regulations to statutes is not the norm in conducting an implied repeal analysis.

Congress should clarify that the most stringent standards to sharing health information apply when an entity is covered by more than one statute.

### **III. CONCLUSION**

In spite of some Congressional action, there remain significant gaps in the protection of the use and disclosure of medical information. Bringing all of those who use and disclose medical information within the bounds of federal law can help close these gaps. Additionally, Congress should require that consumers' permission should be obtained before their medical information is shared with banks, insurers and others. Congress should also clarify that state law that provides a higher degree of protection of medical information is preserved. Enacting such protections would bring the laws in line with what health care consumers need and expect.