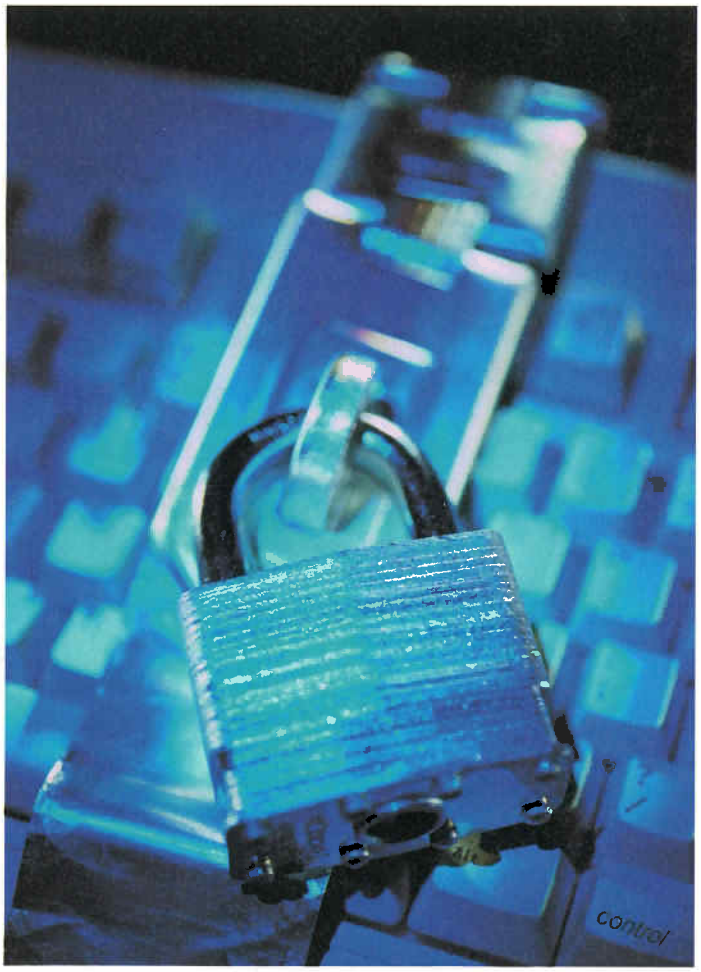
MEDICAL RECORD PRIVACY:

HIPAA And Its Effect on Subrogation

by Gary L. Wickert, Mohr & Anderson, S.C., Hartford, Wisconsin.



A sweeping set of medical privacy laws and regulations enacted recently to give patients unprecedented control over their medical histories and records, have the entire insurance industry scratching its head with regard to the effect they will have on underwriting, claims handling, claims administration, reinsurance, and even subrogation. At the focus of these expansive new regulations are "medical records and other individually identifiable health information held or disclosed by any covered entity, including insurers, in any form, whether communicated electronically, on paper or orally." This article will attempt to identify the legislation and regulations at issue and address how the industry's subrogation practices will be affected by them.

THE PROBLEM: MEDICAL RECORD PRIVACY

Every time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist, or sends a claim to a health plan, a record is made of their confidential health information. Historically, the confidentiality and privacy of those records has been maintained by our family physicians, who kept the records locked away in a file cabinet somewhere within the bowels of their offices and refused to reveal them to anyone else without your written consent.

Times have changed. Today, medical records are zipped around the country with the click of a mouse button, and the use and disclosure of these documents is protected only by a patchwork of state laws, leaving large gaps in the protection of patients' privacy and confidentiality. Former President Bill Clinton repeatedly declared that there was a pressing need for national standards to control the flow of sensitive patient information and to establish real penalties for the misuse or disclosure of this information.

THE SOLUTION: HIPAA'S PRIVACY REGULATIONS

President Clinton and the Republican Congress have long debated the need for national patient record privacy standards. In 1996, however, they enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[1]

1> Pub. L. 104-191, August 21, 1996, 110 Stat. 1936, United States Public Laws.

HIPAA amended the Public Health Service Act (PHSA), the Employee Retirement Income Security Act (ERISA) and the Internal Revenue Code to provide for, among other things, improved portability and continuity of health insurance coverage.

HIPAA also gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. After three years of debate in Congress without passage of such a law, HIPAA provided the Department of Health and Human Services (HHS) with the authority to craft such privacy protections by regulation. Following the principles and policies laid out in the recommendations for national health information privacy legislation which the Administration submitted to Congress in 1997, the Administration drafted regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records and the President and the Secretary Donna E. Shalala released these "privacy regulations" in October 1999. During an extended comment period, HHS received more than 52,000 electronic or paper communications from the public, commenting on these regulations. The final "privacy regulations" were recently published and the 74 pages of regulations and 1,300 pages of comments appeared in the Federal Register on December 28, 2000.[2]

2> 65 F.R. 82462-01, December 28, 2000, 2000 WL 1875566 (F.R.).

These regulations, which will become effective on December 28, 2002, are rumored to carry with them a profound impact on the way health insurers and other insurance companies not only process health and medical related claims, but also subrogate those claims.

THE PROBLEM WITH THE SOLUTION: THE $18 BILLION PANACEA

President Clinton's sweeping set of medical privacy protections, which have as their intent giving patients unprecedented control over their medical histories, will undoubtedly necessitate costly changes in how doctors and hospitals do business, according to medical experts. *The Houston Chronicle* reported on December 20, 2000 that these sweeping changes could result in longer patient visits, additional computer security costs, and the possible financial failure of smaller physicians' practices. *The Houston Chronicle* also reported that these regulations, which do not go into full effect for two years, require doctors to get consent from patients to use medical records in even the most routine matters. They also state that violations of patient privacy can result in fines of up to $250,000.00 or ten years in prison. It is thought that doctors and hospitals may have to make basic changes in day-to-day operations, including additional explanation of protections to patients at the outset of initial visits, resulting in fewer patients seen each day. Costly electronic security software will have to be installed and staff - from doctors to clerical workers - must be trained on what they can and cannot send out of the office, and under what conditions. The White House has estimated that it will cost $17.6 billion nationally and more than ten years to get all of this done, but note that the health insurance industry can offset these costs by transferring the bulk of their paper records to more efficient computer databases. The National Association of Public Hospitals in Washington, D.C. estimates that the cost of retooling computer systems and retraining personnel could cost two to three times as much as it did to put in place Y2K safeguards in late 1999. While it is unclear exactly how the hundreds of pages of HIPAA regulations will improve medical record security and privacy, it is equally uncertain how the new privacy regulations, which were published on December 28, 2000, will affect subrogation efforts of the insurance industry when they involve a health-related claim.

HIPAA'S IMPACT ON SUBROGATION

The impact these new privacy regulations will have on subrogation is unclear from the initial draft of the regulations, and may depend on whether the subrogating carrier is a health insurance carrier or a non-health insurance carrier. To help me sort out the wheat from the chaff, I put in a call to Jody Noon, J.D., R.N. Jody is a partner with the consulting firm of Deloitte & Touche, and heads the Health Information Privacy Services Department at that firm, which has been designated and appointed as consultants to discuss the impact of HIPAA on health care organizations. She can be reached at (503) 727-5207.

"We are still trying to digest it all," says Jody. According to her, both HIPAA and the final privacy regulations are aimed at protecting electronic, oral and paper medical records and other personal health information maintained by health care providers, hospitals, health plans and health insurers, and health care clearinghouses. In short, HIPAA and the privacy regulations should apply only to health insurance carriers. The good news is that the new HIPAA regulations should still allow health insurers to use and disclose individually identifiable health information ("IIHI") for "treatment, payment and health care operations" ("TPO"). Within the regulations, "payment" is defined as:

1)The activities undertaken by:

A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

2) The activities in Paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

Determinations of eligibility of coverage (including coordination of benefits or of a determination of cost sharing amounts), and adjudication or **subrogation of health care claims...**

Section 164.502(e) of HIPAA (which will ultimately be published at 45 C.F.R. §164) indicates that "covered entities" may disclose "IIHI" to business associates who are acting on behalf of the covered entity so long as the business associate agrees, through a written contract that conforms with §164.504(e), to appropriately safeguard the information and only use and disclose the information pursuant to the terms of the agreement with the covered entity. It appears, however, that the regulations do allow the "use and disclosure" of IIHI for "treatment, payment and health care operations" without the need for such a written contract. In short, anyone involved in TPO (which includes subrogation as per the definition of "payment"), is generally authorized to release and transmit medical information and records without specific authorizations signed by the owner of the medical records. Remember, HIPAA applies only to health insurance carriers. Therefore, if you are a subrogating health insurance carrier, it appears that you may not be required to jump through endless hoops in order to comply with these new privacy regulations, according to Jody Noon.

"All of these regulations are targeted at preventing unauthorized (non-normal use) of private medical records, such as for transmission of records to research entities or use of these records to determine life insurance purchasing prospects," she says, adding that it might be possible to simply get yourself "outside of these regulations" by de-identifying the patient in the records (presumably by redacting patient information from the records). However, this is neither practical nor will

Medical Record Privacy ▸ 39

it serve the purpose of a subrogating carrier's transmission of medical records as substantiation of a subrogation claim for purposes of documenting damages and settling with a third party or its carrier.

THE FSMA AND NON-HEALTH INSURANCE SUBROGATION

If only health insurers are governed by the security regulations of HIPAA, what, if anything, regulates the transmission of medical records in the normal course of subrogation for non-health insurance carriers, such as automobile insurers, workers' compensation carriers, etc.? The answer appears to be the Federal Services Modernization Act of 1999 ("FSMA").[3]

3> Pub. L. 106-102, November 12, 1999, 113 Stat. 1338, United States Public Laws, 106th Congress - First Session - (SB 900, Gramm-Leach-Bliley Financial Modernization Act), also known as HIPAA Privacy Regulations.

The FSMA was originally passed in August 1999 and is known as the Gramm-Leach-Bliley Act. It was originally enacted to protect private financial documentation and applied to financial institutions, but was gradually expanded to pull in insurance companies and cover health insurance information as well, according to Jody Noon. The FSMA became effective on November 12, 1999, and its privacy regulations allow for compliance by July 1, 2001. According to Jody Noon, this Act and its medical security regulations are not nearly as onerous as HIPAA's. However, she referred me to Debbi Suoganen, J.D. with Deloitte & Touche. Debbi is with the Health Care Regulatory Group within Deloitte & Touche and is a specialist on the Gramm-Leach-Bliley Act. She can be reached at (714) 436-7319.

"The Gramm-Leach-Bliley Act (GLB) was intended to break down old barriers that kept financial institutions from efficiently sharing information in an electronic world," says Suoganen. "But the GLB talks only of financial information and lumps health care into it. Banks and insurers and security firms are all lumped into one, and lawmakers didn't distinguish between bank records and medical records." As a result, health information could be sold and traded as a financial product without the owners' consent. Is that bad? It depends. A loss of privacy is worth the convenience of being able to access bits and pieces of your life anywhere in the world, such as the use of ATMs. However, such information can often be used for marketing purposes, such as one man who was deluged with telemarketers peddling syringes and insulin after he was diagnosed as a diabetic. As a result of abuses such as these, the FSMA calls for standards of privacy in financial records, and requires the states to adopt privacy standards by November 13, 2000. But the law also had a built-in extended deadline of July 1, 2001, and several states have extended their deadlines to this date. Debbi Suoganen explains that the FSMA was intended to pull together what had been a patchwork of non-uniform state laws on privacy which affected carriers differently from state to state. In October of 2000, the National Association of Independent Insurers (NAIC) voted unanimously to adopt a Model Act for Consumer Financial and Health Information Privacy Regulations. NAIC claims that its Model Act will help states comply with the consumer privacy protections outlined in the FSMA, but some industry groups argue that the Model is unfair to insurers.

Section 17 of the NAIC Model Regulations answers the question of when a medical authorization is required for disclosure of Non-Public Personal Health Information. The NAIC Model Regulations appear to prohibit a licensee from disclosing health care information concerning a consumer or customer unless an authorization is first obtained. The regulations then go on to state what has to be contained in the authorization. However, §17(b) of the NAIC regulations clearly states that nothing in that section will require an authorization for the distribution of Non-Public Personal Health Information by a licensee (insurer) for the purposes of performing a laundry list of insurance functions, including, but not limited to:

1. Claims Administration
2. Claims Adjusting and Management
3. Detection of Fraud
4. Underwriting
5. Reinsurance
6. Excess Loss Insurance
7. Peer Review
8. Research
9. Investigating and Filing Grievances
10. "Where medical record disclosure is required or is one of the lawful or appropriate methods to enforce the licensee's (insurer's) rights or rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer (insured) requests or authorizes."

Debbi Suoganen believes that exception number 10 above includes subrogation activities such as forwarding medical records to third party liability carriers or self-insured entities for purposes of resolving subrogation claims.

Every state has to either adopt the NAIC Model Regulations under the FSMA or come up with their own privacy laws that meet or exceed these standards. Accordingly, it is important for an insurer to look at the particular state in which business is being conducted to determine medical record privacy regulations which they must comply with. At this point, it is too early to tell what any particular state is going to do. The compliance date of July 1, 2001 for the FSMA is a lot closer than the compliance date for HIPAA. Debbi Suoganen explains that if you are a health insurer and comply with HIPAA, you automatically comply with the FSMA. But a non-health insurance company would not want to comply with the more onerous HIPAA regulations, so it will have to comply with the FSMA regulations in less than six months.

SUMMARY

Both HIPAA and FSMA appear to have exceptions and allowances for subrogating carriers to transmit medical records to third party carriers for purposes of resolving subrogation claims. Each act attempts to regulate how medical records may be used and to whom they may be disclosed, and protects such uses and disclosures. Jody Noon provided me with a simple rule: "Ask yourself whether or not the recipient of the medical records needs to know who the patient is - if the recipient does not need to know this information, it is probably a non-normal use of the medical records

Medical Report Privacy 44

39 Medical Report Privacy

and strictly governed somehow by these acts." HIPAA's privacy regulations will not become effective for two years, and the states' full compliance with the FSMA's privacy regulations and procedures will not be required until July 1, 2001. It may be that certain forms and/or policies must be utilized and instituted by insurance companies to ensure compliance with these new regulations, according to Jody Noon. However, it looks like the procedural aspect of transmitting medical records in the ordinary course of business for a subrogating carrier will not be altered dramatically.

There still appear to be more questions than answers. What if a carrier has multiple lines? It will be difficult to have its health insurance lines comply with HIPAA, but other lines comply only with the FSMA. It appears as though the main concern insurers should have with regard to these new health care privacy regulations is how to share information outside of the normal course of business. This includes marketing efforts, crossovers (such as bank owning insurance company), or the internal or external transfer of health care information for anything other than the normal course of insurance business. Advice of counsel should be sought in establishing internal policies and procedures to deal with these concerns. Specific questions regarding the applicability of these acts as well as compliance thereto, may be addressed directly to Jody Noon and/or Debbi Suoganen.

Note: At the time of writing this article the specific language of many of these regulations was not even yet available. The information contained in this article should not be construed or utilized as legal advice specific to a carrier's procedures and compliance with Federal or State law. Such advice should only be sought within the confines of the confidential attorney-client relationship with regard to facts specific to the matter for which consultation is being sought. The information in this article should not be construed or utilized as legal advice in any way.