US Health Data Marketing Rules Fail Privacy Test

Report by Robert Gellman

ON DECEMBER 20TH 2000 the US Health and Human Services Secretary Donna E. Shalala released rules made under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Ms. Shalala stated that the rules were designed to protect the privacy of Americans' personal health records.

She continued: "For the first time, all Americans – no matter where they live, no matter where they get their health care – will have protections for their most private personal information, their health records. With these standards, all Americans will be able to have confidence that their personal health information will be protected."

While some have reacted favourably to elements of these new privacy rules, the marketing rules are not without their critics.

During debates over health privacy proposals, it was often said that video rental records had better privacy protection than medical records. Unfortunately, now that the final HIPAA privacy rules have been issued, it is still true that video rental records have better protections from marketing uses and disclosures than medical records.

PRIVACY WEAKNESSES IN THE MARKETING RULES

• The rules contain the most sweeping authorisation for the use of patient information for marketing proposed in the last twenty years. The marketing rule was not in the draft rule published for comment.

• The rules expressly authorise disclosures for marketing without patient consent. For example, health providers or plans can use information about a woman's pregnancy for marketing and can disclose it to others for marketing. A woman could only object after the fact.

• Providers and payers can use all medical information they hold for marketing without affirmative patient consent or without the patient's opportunity to opt-out in advance.

• All protected health information can be disclosed for marketing. The rules do not protect information about diagnoses, prescriptions, pregnancy, sexually transmitted diseases, mental health treatments, or confidential communications. Marketing to minors or using protected health information about minors is permitted.

• Patients have the right to opt-out of marketing only after receiving a marketing communication. If a family of four has a dozen doctors, clinics, health plans, hospitals, laboratories, pharmacies, pharmacy benefit managers, etc., the family may have to write 48 separate letters to opt-out of each organisation's marketing activities.

• Patients do not have to be offered toll-free numbers to opt-out, the ability to opt-out online, or post-paid opt-out letters. A covered entity could require an individual to send a separate snail mail letter to opt out. Nothing in the rule says that a covered entity cannot charge patients who want to opt-out.

• Health and Human Services has defended the marketing rule by saying that it allows physicians to make recommendations to patients. However, the definition of marketing expressly excludes these recommendations. Therefore, a rule allowing broad uses and disclosures for marketing is not necessary to permit physicians to make treatment recommendations.

RULES PERMIT THIRD PARTY MARKETING

Any doubts about the sweeping scope of the marketing rule is put to rest by these words from the preamble to the rule (page 82771 of the Federal Register notice):

"However, the final rule permits an alternative arrangement: the covered entity can engage in health-related marketing on behalf of a third party, presumably for a fee. Moreover, the covered entity could retain another party, through a business associate relationship, to conduct the actual health-related marketing, such as mailings or telemarketing, under the covered entity's name."

This language says expressly that marketing is permissible for a fee, is permissible on behalf of third parties, and that telemarketing is permissible.

PATIENT AUTHORISATION NOT REQUIRED

A covered entity does not need patient authorisation if it uses or discloses protected health information for marketing under any of these conditions:

1) In a face-to-face encounter with an individual. The encounter does not have to involve a provider. For example, a marketer could knock on the door of a pregnant woman and try to sell her a product or service. Face-to-face marketing using medical information might also be done be for cars, vacations, magazines, or other products or services unrelated to health.

2) If the marketing concerns products or services of nominal value. For example, a hospital might use or disclose a list of patients with a particular diagnosis if the purpose were to distribute a 25-cents off coupon for a product that costs a dollar. The marketing could be for products or services unrelated to health.

3) If the marketing concerns the health-related products and services of the covered entity or of a third party, and the communication meets the applicable conditions (see below).

CONDITIONS FOR HEALTH-RELATED MARKETING OFFER LIMITED PROTECTION

The conditions that apply to the last category of marketing offer some limited protections. The communication must identify the covered entity as the party making the communications. If the information were given to a business associate, the business associate might have to say that it was the covered entity. This may actually hide the fact that the information had been shared with another entity. Or the information might be presented in another way; for example, "now that you are pregnant, your doctor asked us to tell you about our diaper service." Because any covered entity can use data for marketing, the source of the data might be a laboratory or other indirect provider that a patient would not even recognise.

The communication must prominently disclose whether the covered entity was being paid directly or indirectly. This can be done easily. Consider, "The XYZ diaper company is paying us to mail this offer to you, but we think the offer is so wonderful that we would have done it anyway had we thought of it first."

The third condition requires that the patient be given an opportunity to opt-out of receiving future communications. There are several problems here. An opt-out is not required for newsletters or general communications distributed to a broad cross-section of individuals. However, it is not clear what a broad cross-section means. A hospital being paid to send a promotion for a drug manufacturer could avoid offering an opt-out if the communication were to a broad enough group. For example, a promotion for a drug of interest only to diabetics would not have to offer an opt-out if the promotion went to all hospital patients.

OPT-OUT SHORTCOMINGS

It is not clear what is meant by opt-out. Would a patient opting out of a promotion for a diabetes drug also have to opt-out separately of promotions for heart, kidney, and cancer drugs or promotions for other third parties? Would opt-outs cover institutions, business associates, indirect providers and hybrid entities, or would separate opt-outs be required?

The rule does not specify an opt-out procedure. An 800 (toll-free) number for opt-outs is not required. No online opt-out is required. No post-paid opt-out card/letter is required. Patients could be required to write a snail mail letter for each provider, health plan, insurance company, pharmacy, pharmacy benefit manager, laboratory, X-ray facility, clinic, and other facility. "If you want to opt-out of future promotions, write a letter containing your name, address, health plan, SSN, medical record number, the names of your doctors at our hospital, the clinics you attend, and send it to us at….".

Perhaps the worst opt-out feature is that the rule does not provide for opt-in or even advance opt-out. An individual acquires the right to opt-out only after receiving a marketing communication.

PRIVACY-RISK MARKETING WIDELY JUSTIFIED

There are other conditions if a covered entity uses or discloses protected health information to target communications based on health status or condition. The entity must determine that the product is beneficial to the targeted individuals. The rule does not require a determination by a treating physician or health professional. An administrator can presumably make the determination. Any study that shows any potential benefit, no matter how small or questionable, might be enough to justify a determination. For example, the rule might permit the marketing of vacation packages to patients with a variety of ailments or as a preventative measure.

A second condition requires that the communication explain why the individual has been targeted and why the product or service would be beneficial. This condition actually runs the risk of further invading the privacy of marketing subjects. Imagine marketing condoms to a teenager who was treated for syphilis. The promotion would have to say that the teenager was selected because s/he was sexually active and condoms will prevent a recurrence of the disease. What happens if the teenager's parent opens the letter first? A woman who had an abortion that her family did not know about might receive a solicitation for family planning services that mentioned her abortion.

A third condition states that a covered entity must make reasonable efforts to ensure that opt-outs will be honoured. This condition is useful, but the rule does not require anyone to make reasonable efforts to provide easy, free, and alternative opt-out methods. Nor does the rule require that a patient be able to opt-out without paying a fee.

The rule suggests that information

cannot be disclosed to a third party without consent. That is true, but it is misleading. A disclosure for marketing can be made to a business associate, and anyone can become a business associate by signing a contract with a covered entity. Patient records can be disclosed, for example, to a telemarketing firm if the firm becomes a business associate. The telemarketer can then market any health-related product or service, including a product or service of a company that is not a business associate.

The general privacy rules attach to business associates who receive disclosures from covered entities. That is a good thing, but it still permits broad scale marketing using patient information. And business associates could be allowed to make disclosures to their business associates.

The information of a consumer who responds to a promotion might not be covered by the privacy rule, and a consumer who responds to a marketing solicitation might be disclosing name, address, and diagnosis to a third party not covered by the rule. Further use of the information would therefore be unrestricted.

Rights and remedies

Another consequence of the marketing rule concerns remedies available to individuals whose records are misused. The final rule removed the requirement that patients be identified as third party beneficiaries under any contracts with business associates. Thus, if a marketer or business associate of a hospital misuses health information it has received, a patient would have no clear right to sue under the HIPAA scheme. The legal conclusion on this point would vary from state to state, and there remains a great deal of uncertainty about third party beneficiary law and health privacy. Nevertheless, it is possible that the patient would have no remedy.

Video Privacy Protection Act (for comparison)

The Video Privacy Protection Act does not allow video operators to disclose the names of movies that an individual rented unless the individual provides affirmative consent. The HIPAA health privacy rules allow use and disclosure of any protected health information for many marketing purposes without the individual's affirmative consent.

The Video Privacy Protection Act allows video operators to disclose the categories of movies rented (not actual titles) only if an individual was given an opportunity in advance to opt-out. The HIPAA health privacy rules allow disclosure of any protected health information for many marketing purposes without mandating an advance opt-out.

Further information about the HIPAA privacy rules can be found at the Department of Health and Human Services website: http://www.aspe.hhs.gov/admnsimp.

Robert Gellman is a Privacy and Information Policy Consultant, Washington DC, USA. He can be reached at rgellman@cais.com

Continued from page 13

Since the average user is not necessarily familiar with the technical aspects of the Internet, and is not always able to decide on or change the configuration of the hardware and software used, it is crucial that the products' default settings offer the highest level of privacy protection.

Although new technologies are traditionally considered a threat to privacy, they can offer useful ways to safeguard privacy. These "privacy enhancing technologies" minimise or prevent the collection or any further processing of identifiable data. Technology – for example, proxy servers, cookie killers, anonymisation software, pseudonymisation tools and e-mail filters – may also hinder unlawful processing.

4. Build trusted mechanisms for control and feedback

On-line data protection can be effective only if there are adequate means to monitor and evaluate compliance with both the legal framework and technical requirements. Even though Data Protection Authorities are the front line enforcement mechanism, other actors are moving towards self-monitoring as they have realised the impact of their privacy policies on consumer behaviour.

Furthermore, granting privacy "labels" would provide consumers a trustworthy indication of data processing compliance with EU data protection legislation. The Working Party intends to ensure that privacy labels are granted in particular to websites that satisfy European data protection legislation.

This report is based on the briefing note provided to the European Parliament to support Peter Hustinx's presentation at the seminar. Both the report and the briefing note were written by Diana Alonso Blas, Senior International Officer, Dutch Data Protection Authority (Registratiekamer). E-mail: dal@registratiekamer.nl