BNA's
HEALTH LAW REPORTER
BNA Employee-Owned Since 1947

Reproduced with permission from BNA's Health Law Reporter, Vol. 11, No. 31, 08/01/2002, pp. 1125-1132. Copyright © 2005 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

# Health Care Privacy, Bioterrorism Preparedness, and Other Challenges For Health Care Providers in the Post-September 11th World

BY MARK BARNES, BRIAN M. WYATT, CLINTON D. HERMES, AND KIMBERLEE A. CLEAVELAND[1]

Like all other industries, health care is facing a new reality in the wake of the terrorist attacks on Sept. 11, 2001. From the increased focus on disaster planning and readiness, as evidenced by, among other things, the new standards published by the Joint Commission on Accreditation of Healthcare Organizations (''JCAHO'') in November 2001, to already thinly staffed facilities dealing with greater personnel shortages as reservists with medical experience have been called to military service, the operational, legal, and economic issues facing health care providers across the country are increasingly numerous and complex.

In the midst of these changes, the federal government has taken substantial steps to enhance its ability to combat terrorism, both in the United States and abroad. Some of these steps will confront health care providers with difficult decisions as they try to fulfill their patient care, educational, and research missions. They must remain sensitive to increased public health and national security concerns, while protecting the privacy and confidentiality of health information, in particular as required by the Standards for Privacy of Individually Identifiable Health Information[2] (the ''Privacy Rule'') promulgated under the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (''HIPAA'').

This article is intended to highlight some of the most pressing of these issues. First, we discuss certain provisions of the Privacy Rule that might apply in the event that a health care provider that is a ''covered entity'' (as defined in the Privacy Rule) (referred to herein as a ''provider'') is faced with deciding whether it is permitted to disclose ''protected health information'' (as defined in the Privacy Rule) (''PHI'') without the consent or authorization of the individual subject when responding to, or attempting to prevent, acts of terrorism. Second, we briefly summarize certain provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001[3] (the ''USA PATRIOT Act'') that are pertinent to providers, paying particular attention to how providers may comply with the USA PATRIOT Act without violating the Privacy Rule. Finally, we briefly summarize some of the current federal and state legislation aimed at in-

[1] *Barnes is a partner with Ropes & Gray in New York. Wyatt, Hermes, and Cleaveland are associates with the firm. Barnes can be reached at MBarnes@ropesgray.com, or (646) 840-6835. Wyatt can be reached at BWyatt@ropesgray.com, or (646) 840-6836. Cleaveland can be reached at KCleaveland@ropesgray.com, or (617) 951-7032. The authors would like to thank Jason A. Rantanan for his assistance in preparation of this article.*

[2] 65 Fed. Reg. 82,462 *et seq.* (Dec. 28, 2000) (to be codified at 45 C.F.R. Parts 160 and 164).

[3] 107 P.L. 56, 115 Stat. 272 (Oct. 26, 2001).

COPYRIGHT © 2002 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C. 20037 ISSN 1064-2137

creasing preparedness for, and reducing the threat of, bioterrorism in the United States.

## Uses, Disclosures of PHI Under the Privacy Rule

The Privacy Rule constitutes the first attempt by the federal government to comprehensively regulate the privacy of PHI. The Privacy Rule's baseline is that a covered entity may not use or disclose an individual's PHI without the individual's (or the individual's personal representative's) written consent[4] or authorization unless an exception applies. In this article, we highlight a number of provisions under the Privacy Rule that would permit health care providers to disclose PHI without individual consent or authorization when responding to, or attempting to prevent, terrorist activities.

It is important to note that while certain uses and disclosures may be permitted under the Privacy Rule, they still may be prohibited under state law.[5] In addition, the Privacy Rule in many instances will require that providers make all reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose of the use or disclosure (colloquially referred to as the ''minimum necessary rule'').[6] The Privacy Rule also requires that, in most cases, providers verify the identity and authority of persons requesting PHI, and that they secure certain documentation when making disclosures pursuant to the Privacy Rule.[7] Accordingly, before using or disclosing PHI for any of the purposes discussed herein, health care providers should consult with their legal counsel regarding the effect of applicable state law, the minimum necessary rule, requirements for proper verification of the identity and authority of the party to whom disclosure is to be made, and other considerations, legal and otherwise, applicable to the specific circumstances.

### ■ *Disclosures Required by Law*

Under the Privacy Rule, providers are permitted to use or disclose an individual's PHI without consent or authorization to the extent required by law, so long as the disclosure complies with, and is limited to, the relevant requirements of that law.[8] However, disclosures of PHI that are required by law but are made in the course of judicial or administrative proceedings, or for law enforcement purposes, are subject to additional protective requirements under the Privacy Rule, as highlighted below.[9]

### ■ *Public Health Activities*

Under the Privacy Rule, a provider may disclose an individual's PHI without consent or authorization to authorized public health authorities for the purpose of preventing or controlling disease, injury, or disability.[10] A provider also may disclose PHI to a person who may have been exposed to a communicable disease (such as smallpox) if it is authorized by law to do so as part of a public health intervention or investigation.[11]

State laws are critical in this context because they establish which disclosures are ''authorized by law.'' In the wake of the events of Sept. 11th and the subsequent appearance of anthrax-laced letters, there has been an effort to modify state public health laws to make them more workable in the face of actual bioterrorism threats. This is spearheaded by The Model State Emergency Health Powers Act (the ''MSEHPA''), which was initially published on Oct. 23, 2001, and then modified and republished on Dec. 21, 2001.[12] The MSEHPA was written for the Centers for Disease Control and Prevention[13] (''CDC'') primarily by academics at the Center for Law and the Public's Health at Georgetown and Johns Hopkins universities.

The MSEHPA would allow a governor to declare a public health emergency and to assume broad powers during that emergency. These powers would include the ability to compel quarantines, condemn property, and require health care workers to assist with the medical response to the public health emergency or potentially lose their licenses. Since its initial publication a few states have passed the substantive elements of the MSEHPA.[14] While several other states are currently considering it, the MSEHPA has received extensive criticism from various civil liberties groups and in the press.[15] For this reason, a number of states have passed

---

[4] Consent only covers the use and disclosure of PHI for treatment, payment and health care operations, as described in the provider's notice of privacy practices. 45 C.F.R. § 164.506. The U.S. Department of Health and Human Services proposed modifications to the Privacy Rule that would eliminate the requirement that health care providers obtain this written consent before using or disclosing the individual's PHI for these purposes. 67 Fed. Reg. 14,778-14,781 (March 27, 2002). If the proposed modifications are promulgated in a final rule, health care providers will be permitted, but not required, to obtain the individual's written consent to use and disclose PHI for treatment, payment and health care operations.

[5] The regulations promulgated under HIPAA, including the Privacy Rule, will preempt a contrary provision of a state law regarding health information privacy unless that provision of state law is more stringent in protecting the privacy of an individual's PHI, in which case the state law would survive preemption and compliance with the applicable provisions of the HIPAA regulations and state law would be required. If the provision of state law is not contrary to the HIPAA regulations, it may be necessary to comply with both the provision of state law and the HIPAA regulations. 45 C.F.R. Part 160, Subpart B. For further information on conducting a HIPAA preemption analysis, *see* M. Barnes, et al., ''The HIPAA Privacy Rule: A Guide To Conducting State Law Preemption Analyses,'' *BNA's Health Law Reporter*, Vol. 11, No. 18 (May 2, 2002).

[6] 45 C.F.R. §§ 164.502(b) and 164.514(d). The minimum necessary rule does not apply to, *inter alia*, (i) disclosures of PHI to, and requests for PHI by, a health care provider for treatment, and (ii) uses and disclosures of PHI that are ''required by law'' (as discussed further below).

[7] 45 C.F.R. § 164.514(h).

[8] 45 C.F.R. § 164.512(a).

[9] *See* discussion of disclosures for *Judicial And Administrative Proceedings* and *Law Enforcement Purposes* below.

[10] 45 C.F.R. § 164.512(b).

[11] *Id.*

[12] The MSEHPA is available at http://www.publichealthlaw.net/.

[13] Other sponsors include the National Governors Association, the National Conference of State Legislatures, and the National Association of Attorneys General.

[14] Among these states are Minnesota (Minn. H.F. 3031 (signed by Gov. Jesse Ventura (I) on May 22, 2002)) and Tennessee (Tenn. S.B. 2392 (signed by Gov. Don Sundquist (R) on May 22, 2002)).

[15] Kristin Choo, *Controversial Cure*, ABA JOURNAL (April 2002); Duane Parde, *CDC proposal is extreme*, USA TODAY (April 25, 2002).

 COPYRIGHT © 2002 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C.  ISSN 1064-2137

only limited versions of the MSHEPA.[16] Likewise, in a few states, including Mississippi and Wyoming, proposed legislation based upon the MSEHPA has been completely defeated. In Massachusetts, no action has been taken on the MSEHPA bill since late November 2001. Because the content and status of the laws and legislation based on the MSHEPA varies greatly from state to state, as do the public health laws that pre-date the MSHEPA, disclosures permitted for authorized public health purposes under HIPAA will vary as well.

In addition, a provider may disclose PHI to an individual's employer without the individual's consent or authorization if the provider delivers health care to the individual to assist with the employer's recording or other medical surveillance responsibilities under federal or state law, as long as the provider has given written notice to the individual that such disclosure may occur. For example, the Privacy Rule would permit a provider to disclose to an employer that one of its employees has contracted an infectious disease after having been asked by that employer to evaluate the employee for a work-related illness, if the employer needs that information in order to comply with its recording or other medical surveillance responsibilities under the law.[17]

## ■ *Disclosures to Notify, Locate, or Identify People Responsible for Individual's Care*

Under the Privacy Rule, a provider may use or disclose PHI about an individual in order to notify or assist in notifying (including identifying or locating) a family member, personal representative, or other person responsible for the individual's care about the individual's location, general condition or death.[18] In most cases, a provider must obtain the individual's verbal permission (or at least provide the individual with an opportunity to object) to such use and disclosure of his or her PHI. If the individual is not present or is otherwise unavailable (*e.g.*, because of incapacity or medical emergency) the provider may only use or disclose PHI if it determines that doing so is in the best interests of the individual; additionally, any such disclosure must be limited to that PHI that is directly relevant to the recipient's involvement in the individual's health care.[19]

Similarly, in the event of a disaster—such as an airplane crash or terrorist bombing—a provider may use, or disclose to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, an individual's PHI in order to coordinate disclosures to notify or assist in the notification of (including identifying or locating) a family member, personal representative, or other person who is responsible for the individual's care about the individual's location, condition or death.[20] The requirements outlined above relating to obtaining the individual's prior verbal permission also apply to disaster relief disclosures to the extent the provider determines that such requirements do not interfere with its ability to respond to the emergency circumstances.[21]

## ■ *Judicial and Administrative Proceedings*

Under the Privacy Rule, a provider may disclose PHI in response to an order of a court or administrative tribunal in the course of any judicial or administrative proceeding, provided that only the PHI expressly authorized by the order is disclosed.[22] A provider also may disclose an individual's PHI in response to a subpoena or discovery request that is *not* accompanied by a court order if it receives certain assurances from the requesting party that efforts have been made to inform the individual of the request or to obtain a court order protecting the information from further disclosure.[23] Providers may be faced with deciding whether to disclose PHI under this exception when the United States proceeds with criminal prosecution of terrorists.

## ■ *Law Enforcement Purposes*

Under the Privacy Rule, providers may disclose PHI to law enforcement officials,[24] including those who are attempting to combat terrorism, under the following circumstances:

- A provider may disclose PHI to law enforcement officials as required by law, including laws that require the reporting of certain types of wounds or other physical injuries. However, disclosures concerning victims of abuse, neglect or domestic violence do not qualify for this exception and are subject instead to the requirements of Sections 164.512(b)(1)(ii) and 164.512(c)(1) of the Privacy Rule.[25]
- A provider may disclose PHI to law enforcement officials in compliance with, and as limited by, a court order, a court-ordered warrant, or a subpoena or summons issued by a judicial officer or a grand jury.[26]
- A provider may disclose to law enforcement officials PHI pursuant to an administrative subpoena, summons, or other request provided that the information sought is relevant and material to a legitimate law enforcement inquiry, the request is specific and limited in scope to the extent reasonably practicable, and de-identified information could not reasonably be used.[27]
- Unless further disclosure is permitted under the categories discussed above, in response to a law enforcement official's request to identify or locate a suspect, fugitive, material witness, or missing person, a provider may disclose only certain limited identifying PHI.[28]

---

[16] These states include Georgia (GA S.B. 385 (signed by Gov. Roy E. Barnes (D) on May 16, 2002)) and New Hampshire (NH H.B. 1478 (signed by Gov. Jeanne Shaheen (D) on May 17, 2002)).

[17] 45 C.F.R. § 164.512(b)(1)(v).

[18] 45 C.F.R. § 164.510(b).

[19] 45 C.F.R. § 164.510(b)(3).

[20] 45 C.F.R. § 164.510(b)(4).

[21] *Id.*

[22] 45 C.F.R. § 164.512(e).

[23] *Id.* For a more detailed explanation of the required assurances, *see* 45 C.F.R. § 164.512(e)(1).

[24] ''Law enforcement official'' means ''an officer or employee of any agency or authority of the United States, a State . . ., [or] a political subdivision of a State . . . who is empowered by law to . . . (1) [i]nvestigate or conduct an official inquiry into a potential violation of law; or (2) [p]rosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.'' 45 C.F.R. § 164.501.

[25] 45 C.F.R. § 164.512(f)(1)(i).

[26] 45 C.F.R. §§ 164.512(f)(1)(ii)(A) & (B).

[27] 45 C.F.R. § 164.512(f)(1)(ii)(C).

[28] 45 C.F.R. § 164.512(f)(2). Such disclosure is limited to name and address, date and place of birth, Social Security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death (if applicable), and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, and the

- A provider may disclose to law enforcement officials PHI about a victim of crime in response to a law enforcement official's request if the victim agrees to the disclosure. Under certain specified conditions, a provider also may disclose a victim's PHI when it is unable to obtain the victim's agreement because of his or her incapacity or other emergency circumstance.[29]
- A provider may disclose to a law enforcement official PHI about a deceased individual if the provider has a suspicion that the individual's death may have resulted from criminal conduct.[30]
- A provider may disclose to law enforcement officials PHI that the provider believes in good faith constitutes evidence of criminal conduct that occurred on its premises.[31]
- A provider may disclose PHI to law enforcement officials in an offsite medical emergency (*e.g.*, emergency medical technicians at the scene of a crime) if necessary to alert law enforcement to the fact that a crime has been committed, unless the medical emergency is the result of abuse, neglect, or domestic violence of an individual in need of emergency health care.[32]

### ■ *Serious Threat to Health or Safety*

Under the Privacy Rule, a provider may use or disclose PHI (consistent with applicable law and standards of ethical conduct) without an individual's consent or authorization if the provider believes in good faith that doing so is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and that such disclosure is made to a person reasonably able to prevent or lessen the threat.[33] Providers also may disclose the minimum PHI necessary to alert law enforcement officials that an individual has escaped from a correctional institution or from lawful custody.[34]

If an individual admits his or her participation in a violent crime that a provider reasonably believes may have caused serious physical harm to a victim, the provider may disclose the individual's statement and certain limited identifying PHI if it believes in good faith that doing so is necessary for law enforcement authorities to identify or apprehend an individual.[35] However, such disclosure may not be made if the individual's admission was made in the course of treatment to affect the propensity to commit the criminal conduct, or counseling or therapy.[36]

### ■ *Specialized Government Functions*

Finally, under a the Privacy Rule, a provider may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities authorized by the National Security Act[37] and implementing authority (*e.g.*, Executive Order 12333).[38] This exception may become increasingly important as the United States strives to collect information to improve its counterintelligence and national security in the wake of the terrorist attacks of Sept. 11th.

## New Authority Under The USA PATRIOT Act

The USA PATRIOT Act provides law enforcement and other federal officials with numerous new or enhanced tools to combat terrorism. We highlight below some of the provisions that may impact the operations of health care providers and, where appropriate, we examine how health care providers may comply with requests for information made pursuant to the USA PATRIOT Act without violating the Privacy Rule.

### ■ *Access to Records Under the Foreign Intelligence Surveillance Act*

Section 215 of the USA PATRIOT Act amends Title V of the Foreign Intelligence Surveillance Act of 1978[39] to provide that the director of the Federal Bureau of Investigation may apply for a court order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation is not of a ''United States person'' (which likely includes a U.S. citizen or permanent resident alien, and U.S. corporations) conducted solely on the basis of activities protected by the First Amendment to the Constitution (*e.g.*, free speech rights). Previously, the FBI could only seek this type of order to obtain records from a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility.

A person who, in good faith, produces documents or other tangible things under an order issued pursuant to Section 215 of the USA PATRIOT Act will not be liable to any other person for doing so. Moreover, under the Privacy Rule, a health care provider receiving such an order would be permitted to disclose documents containing PHI without an individual's consent or authorization because an FBI officer conducting such an investigation would qualify as a law enforcement official to whom disclosures may be made in compliance with, and as limited by the relevant requirements of, a court order.[40] Accordingly, a provider should be able to disclose PHI in response to a court order obtained pursuant to Section 215 of the USA PATRIOT Act without risk of liability under the Privacy Rule or otherwise.

### ■ *Interception of Computer Trespasser Communications*

Section 217 of the USA PATRIOT Act amends the federal wiretap statute[41] so that victims of computer attacks may authorize persons ''acting under color of law'' to monitor trespassers on their computer systems. ''Computer trespasser'' includes anyone who accesses a

presence or absence of facial hair, scars, and tattoos. 45 C.F.R. § 164.512(f)(2)(i). Notably, health care providers may *not* disclose PHI related to the individual's DNA, dental records, body fluids, or tissue. 45 C.F.R. § 164.512(f)(2)(ii).

[29] 45 C.F.R. § 164.512(f)(3).
[30] 45 C.F.R. § 164.512(f)(4).
[31] 45 C.F.R. § 164.512(f)(5).
[32] 45 C.F.R. § 164.512(f)(6).
[33] 45 C.F.R. § 164.512(j).
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] 50 U.S.C. 401 *et seq.*
[38] 45 C.F.R. § 164.512(k)(2).
[39] 50 U.S.C. 1861 *et seq.*
[40] *See* 45 C.F.R. § 164.512(f).
[41] The federal wiretap statute is codified at 18 U.S.C. 2510 *et seq.*

 COPYRIGHT © 2002 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C. HLR ISSN 1064-2137

protected computer[42] without authorization, but excludes any person ''known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the protected computer.''[43] Thus, an employee or independent contractor of a provider authorized to access the provider's computer systems would not qualify as a ''computer trespasser,'' but a former employee or independent contractor might.

Before monitoring can occur, certain requirements must be met, one of which is that investigators may intercept only the communications sent or received by the computer trespassers. Consequently, monitored computers must be configured to allow the interception of communications to and from the trespasser without permitting the interception of communications by nonconsenting users who are properly authorized to use the computer. Specifically, a health care provider would need to establish appropriate safeguards to prevent law enforcement officials from accessing or intercepting any communications not sent or received by the computer trespasser.

Moreover, because of the requirements of the Privacy Rule, providers should proceed cautiously when considering whether to invite law enforcement officers to monitor their computer systems as provided in the USA PATRIOT Act. In general, a provider covered by the Privacy Rule should limit law enforcement's access to PHI to the extent possible, and to the extent that establishing firewalls to protect PHI in this manner is not feasible, consider seeking written authorization from individuals whose PHI may be accessed by or otherwise disclosed to law enforcement authorities during monitoring of the provider's systems.

## ■ *Disclosure of Educational Records*

Section 507 of the USA PATRIOT Act amends the Family Educational Rights and Privacy Act[44] (''FERPA'') which protects the privacy of student education records. Section 507 allows the Attorney General and certain other federal officers to apply for a court order requiring an educational agency or institution covered by FERPA to permit the Attorney General to (i) collect education records in the agency or institution's possession, if the records are relevant to an investigation or prosecution of an act of terrorism, and (ii) retain, disseminate and use education records in connection with an investigation or prosecution of an act of terrorism.

Because ''education records,'' as well as certain medical records covered by FERPA that are not ''education records,'' are specifically carved out of the definition of ''protected health information'' in the Privacy Rule,[45] a provider that qualifies as an educational agency or institution under FERPA and that has treated its records as being covered by FERPA would be able to comply with a court order issued pursuant to Section 507 without concern that it will incur liability under the Privacy Rule for that disclosure. The provider may take further comfort from the USA PATRIOT Act's provision that an educational agency or institution that, in good faith, produces education records in accordance with an order issued under Section 507 will not be liable for doing so.

## ■ *Prohibition Against Harboring Terrorists*

Section 803 of the USA PATRIOT Act creates a new offense of harboring or concealing persons who have committed or are about to commit a variety of terrorist offenses, including destruction of aircraft or aircraft facilities, use of nuclear materials or chemical or biological weapons, use of weapons of mass destruction, arson or bombing of government property, destruction of energy facilities, sabotage of nuclear facilities, or aircraft piracy.[46]

A health care provider that suspects that an individual is a terrorist must weigh this new prohibition on harboring terrorists against the requirements of the Privacy Rule when determining whether to disclose to law enforcement authorities information about a suspected terrorist that includes PHI. As noted above, disclosures of PHI without an individual's consent or authorization may be permissible under the Privacy Rule under certain limited circumstances, including if the provider believes in good faith that such disclosure is necessary to avert a serious threat to the public's health or safety. While any such disclosure must be consistent with applicable law and standards of ethical conduct, in most instances disclosure of the identity of a suspected terrorist to law enforcement officials would be permitted. However, providers should keep in mind that the Privacy Rule's minimum necessary rule will apply, absent a court order for additional information or some alternative legally mandated reporting requirement. Moreover, in cases where the suspected terrorist activity is identified through an individual's admission to a provider of his or her participation in the crime, the Privacy Rule limits the PHI that may be disclosed to the statement admitting participation in the crime and limited identifying information about the individual.

## ■ *Expansion of the Biological Weapons Statute and New Duties for Certain Health Care Providers*

The Biological Weapons Anti-Terrorism Act of 1989[47] criminalizes the development, production, stockpiling, transfer, acquisition, retention or possession of biological weapons and delivery systems for biological weapons, as well as the knowing assistance of a foreign state or any organization, threat, attempt or conspiracy to do the same. Section 817 of the USA PATRIOT Act expands the reach of the Biological Weapons Anti-Terrorism Act in the following respects:

- It expands the definition of biological weapons to include any biological agents, toxins, or delivery systems used for purposes other than prophylactic, protective, bona fide research, or other peaceful purposes.
- It criminalizes the knowing possession of any biological agent, toxin, or delivery system of a type or in a quantity

[42] A ''protected computer'' is any computer used in interstate or foreign commerce; any computer connected to the Internet would probably qualify. *See* DOJ Field Guidance on New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation 11 n.4, *available at* http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf (last visited June 14, 2002).

[43] 18 U.S.C. § 2510.

[44] 20 U.S.C. § 1232g.

[45] 45 C.F.R. § 164.501 (definition of ''protected health information'').

[46] This new offense is codified at 18 U.S.C. § 2339.

[47] 18 U.S.C. § 175 *et seq*.

that is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose.[48]

- It adds a new section prohibiting certain ''restricted persons'' (including nationals of specified countries)[49] from ''shipping, transporting or possessing in (or affecting) interstate or foreign commerce any biological agent or toxin, or receiving any biological agent or toxin that has been shipped or transported in interstate or foreign commerce,'' if the biological agent or toxin is listed as a ''select agent'' by the secretary of the U.S. Department of Health and Human Services (''HHS'').[50]

Health care providers that possess biological agents or toxins should consider taking the following steps to reduce potential exposure under Section 817. First, providers should inventory their biological agents and toxins, and carefully manage that inventory, to make certain that they can reasonably justify their retention of those substances based upon a prophylactic, protective, bona fide research, or other peaceful purpose. Second, if a provider possesses any ''select agent,'' it should increase its employee background checking procedures to make certain that no employee who may use or have access to the select agent is a ''restricted person.'' Third, providers must assess, and as necessary enhance, their physical and information technology security with respect to select agents and data about select agents.

It is critical that providers commence these compliance efforts immediately, as the HHS Office of Inspector General (''OIG'') has already indicated that it intends to commence reviews of academic medical centers in the very near future to determine compliance with these provisions of the USA PATRIOT Act. While the OIG's primary focus will be on restricting access of persons from the seven named countries, it may also evaluate compliance with other provisions of the USA PATRIOT Act.

## ■ *Establishment of The First Responders Assistance Act*

Section 1005 of the USA PATRIOT Act enacts ''The First Responders Assistance Act'' authorizing the Attorney General to make grants to states and units of local government to improve the ability of state and local law enforcement, fire departments, and first responders to respond to and prevent acts of terrorism, with $25,000,000 authorized to be appropriated for each of the fiscal years 2003 through 2007. ''Terrorism prevention grants'' may be used for programs, projects, and other activities to, among other things, purchase equipment for responding to and managing a critical incident, including protective equipment for patrol officers such as quick masks. ''Antiterrorism training grants'' may be used for programs, projects, and other activities to address, among other things, critical incident management for all forms of terrorist attack. To obtain a grant, each eligible entity must submit an application to the attorney general.

Although the term ''first responder'' is not defined in the USA PATRIOT Act, usage of that term in other federal statutes and regulations suggests that some providers (particularly ambulance companies and possibly hospitals that operate emergency rooms) could come within its ambit. Accordingly, in looking to defray the significant costs associated with disaster response and bioterrorism preparedness planning, providers that offer first responder services, such as ambulance or other emergency medical services, or operate an emergency department may wish to investigate the availability of funds under the First Responders Assistance Act, once actual appropriations have been made for this purpose. These moneys will be appropriated beginning in fiscal year 2003.

## ■ *Crimes Against Charitable Americans*

Section 1011 of the USA PATRIOT Act responds to fraudulent charity scams that arose in the wake of the Sept. 11th terrorist attacks in several ways. First, Section 1011 amends the Telemarketing and Consumer Fraud and Abuse Prevention Act[51] to cover fraudulent charitable solicitations. It requires that the Federal Trade Commission (the ''FTC'') adopt a rule pursuant to that legislation stating that any person engaged in telemarketing for the solicitation of charitable contributions, donations, or gifts promptly and clearly disclose that this is the purpose of the call, and make such other disclosures as the FTC considers appropriate, including the name and mailing address of the charitable organization on behalf of which the solicitation is made. Providers that solicit charitable contributions or gifts covered by the Telemarketing and Consumer Fraud and Abuse Prevention Act will be required to comply with the FTC's current Telemarketing Sales Rule[52] and any new rules promulgated pursuant to Section 1011 of the USA PATRIOT Act.

Second, Section 1011 amends Section 917 of Title 18 of the United States Code—which prohibits falsely impersonating a member or agent of the American National Red Cross for the purpose of soliciting, collecting, or receiving money or material—to increase the maximum term of imprisonment to five years, making violation of that section a felony (and thereby increasing the maximum fine to $250,000).

Third, Section 1011 amends the Senior Citizens Against Marketing Scams Act[53] to apply to any plan, program, promotion or campaign that is conducted to induce a charitable contribution, donation or gift by use of interstate telephone calls. Under this law, partici-

---

[48] This does not, however, include a biological agent or toxin that is in its naturally occurring environment if it has not been cultivated, collected, or otherwise extracted from its natural source.

[49] Section 817 defines ''restricted persons'' to include any individual who: (i) is under indictment for, or has been convicted in any court of, a crime punishable by imprisonment for a term exceeding one year, is a fugitive from justice, or is an unlawful user of any controlled substance; (ii) is an alien illegally or unlawfully in the United States, or is an alien (other than an alien lawfully admitted for permanent residence) who is a national of a country that the Secretary of State has determined has repeatedly provided support for acts of international terrorism (currently this includes Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria); (iii) has been adjudicated as a mental defective or has been committed to any mental institution; or (iv) has been discharged from the Armed Services of the United States under dishonorable conditions.

[50] This new section is codified at 18 U.S.C. § 175b. It does not apply if such biological agent or toxin is in its naturally-occurring environment and has not been cultivated, collected or otherwise extracted from its natural source.

[51] 15 U.S.C. 6101 *et seq.*

[52] 16 C.F.R. Part 310.

[53] 18 U.S.C. § 2325 *et seq.*

 COPYRIGHT © 2002 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C. HLR ISSN 1064-2137

pants in a scheme that fraudulently solicits charitable contributions or donations may be subject to enhanced penalties for telemarketing fraud under Section 2325 of Title 18 of the United States Code, and mandatory restitution under Section 2327 of Title 18 of the United States Code, even if they do not require the prospective victim to purchase other goods or services. Health care providers that solicit charitable contributions or gifts now may be covered by the provisions of this law.

Accordingly, health care providers (and their development and fundraising offices) engaged in charitable fundraising should review and modify their fundraising practices as necessary to comply with these amended laws.

### ■ *Sense of the Senate Concerning Bioterrorism Preparedness and Response*

A ''Sense of the Senate'' reflects the opinion of the U.S. Senate, but does not carry the force of law. As such, it should be taken only as an indicator of bills that might be approved by the Senate in the future. In Section 1013 of the USA PATRIOT Act, the Senate made findings that greater resources must be provided to increase the capacity of hospitals and local health care workers to respond to public health threats, and that health care professionals must be better trained to recognize, diagnose and treat illnesses arising from biochemical attacks. Given these findings, it is the Senate's opinion that the United States should make substantial new investments in combating bioterrorism, including (i) improving state and local preparedness capabilities by upgrading state and local surveillance epidemiology, assisting in the development of response plans, assuring adequate staffing and training of health professionals to diagnose and care for victims of bioterrorism, extending the electronics communications networks and training personnel, and improving public health laboratories, and (ii) improving hospital response capabilities by assisting hospitals in developing plans for a bioterrorist attack and improving the surge capacity of hospitals. In sum, this Sense of the Senate is a sign that the Senate may look favorably upon bills aimed at improving the ability of health care entities to identify and respond to acts of bioterrorism.

## Federal and State Bioterrorism Legislation

The federal government recently took steps to mitigate the threat of bioterrorism by passing legislation that will impact many hospitals and other health care providers. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002[54] (the ''Bioterrorism Act'') was recently approved by both the House of Representatives and the Senate and signed into law by President Bush on June 12, 2002. The Bioterrorism Act consists of five major parts: (i) a medical and public health response to bioterrorism; (ii) new requirements for regulations regarding the possession and use of biological agents and toxins; (iii) new procedures to protect the food supply; (iv) measures to protect the water supply; and (v) appropriations designed to increase the number of available new drugs. Of particular interest to providers are the appropriations for state and local bioterrorism preparedness and the regulations regarding biological agents and toxins.

[54] P.L. No. 107-188, 116 Stat. 594 (June 12, 2002).

### ■ *Funds for State and Local Bioterrorism Preparedness*

The Bioterrorism Act provides several potential sources of funds for health care providers to use to develop responses to bioterrorism and other public health emergencies. The Bioterrorism Act authorizes the appropriation of a number of different funding sources to combat bioterrorism, including:

- $1.15 billion for the National Pharmaceutical Stockpile, creating a reserve of anti-bioterror drugs and vaccines, including $640 million for smallpox vaccine;
- $300 million for the CDC to upgrade and renovate their facilities; and
- $1.6 billion in grants for states to improve their ability to respond to bioterrorism, including $520 million to enhance hospital preparedness in 2003.

The funds allocated for bioterrorism response can be reached in a number of ways. First, the Bioterrorism Act authorizes the HHS secretary to make grants to health and educational entities to train individuals for professions where there is a shortage that should be alleviated in order to respond effectively to bioterrorism or other public health emergencies.[55]

Second, the HHS secretary is authorized to make block grants to improve the preparedness of states, localities and hospitals.[56] These block grants are made directly to each state in response to an approved bioterrorism and public health emergency preparedness and response plan. These funds may be used by the states for such purposes as to develop statewide coordination and response plans, to purchase or upgrade equipment, and to train health care personnel to detect and respond to biological agents. The use of these funds must relate to bioterrorism, acute outbreaks of infectious diseases, or other public health threats or emergencies. Because these allocations are made directly to the states in the form of block grants, health care providers wishing to apply for these funds should open a dialogue with their respective state governments.

Finally, the Bioterrorism Act allows the HHS secretary to make grants to partnerships consisting of hospitals or other health care facilities, local political subdivisions, and states for the purpose of improving community and hospital preparedness for bioterrorism and other public health emergencies.[57] To be eligible for these grants, a partnership must include at least one member from each category. The funds allocated by these grants may be used for all the purposes for which the state block grants may be used, as well as to prepare triage and transportation plans and train health care personnel to respond to large numbers of people exposed to bioweapons. As with the state block grants, the use of these funds must be related to bioterrorism or other public health threats. Health care providers interested in accessing these funds should enter into a partnership with their local community and state governments.

### ■ *Toxin Regulation and Registry*

In addition to providing funds for state governments and health care providers, the Bioterrorism Act also es-

[55] H.R. 3448, § 106.
[56] H.R. 3448, § 131.
[57] H.R. 3448, § 131.

tablishes new regulations for the use, possession, and transfer of biological agents and toxins.[58] Specifically, it requires the HHS secretary to create a list of biological agents and toxins that have the potential to pose a severe threat to public health and safety. The Bioterrorism Act also requires the promulgation of regulations governing the possession and use of the biological agents and toxins on the list. These regulations will require persons who possess, use, or transfer any of the listed products to register with the HHS secretary and will impose certain restrictions on the use of these materials. A registered person may only grant access to these biological agents or toxins to persons with a legitimate need to handle them and must submit information to the government on each person who handles or uses the materials. The registered person must also deny access to individuals whom the United States Attorney General has designated as ''restricted persons.'' The end result of these regulations will be greater scrutiny and oversight of the people and organizations that handle these biological agents or toxins.

For health care providers, particularly academic medical centers that have substantial research operations in which biological agents or toxins are used, the Bioterrorism Act creates an additional layer of federal regulatory oversight and requires stricter management of the research operations in which such biological agents or toxins are used. Moreover, some states also are moving to require registration to possess or maintain biological agents. For example, North Carolina House Bill 1472, which was signed into law on Nov. 28, 2001, and took effect Jan. 1, 2002, directs the North Carolina Department of Health and Human Services to establish a biological agents registry and a system for safeguarding listed biological agents, and imposes civil penalties for violation of the registry requirements (9 HCPR 1783, 12/3/01).

As discussed above, several of the provisions of the Bioterrorism Act authorize the appropriation of funds that have the potential to offset some of the substantial expenses health care providers already are incurring with respect to disaster planning and bioterrorism preparedness. Notably, these funds already will already be available either indirectly through block grants to states that will eventually make their way to providers, or more directly through grants available to hospitals that are part of consortia that include both a political subdivision of a state and a department of public health. Health care providers—either directly or through their state associations—should promptly open dialogues with the appropriate state officials about how these funds can be made most readily available to the facilities that need them to carry out this critical work.

Finally, it should be noted that certain funds have already been appropriated to fund the Bioterrorism Act's authorized spending. On Jan. 10, 2002, the Department of Defense Appropriations Act for 2002[59] (the ''DOD Act'') was signed into law. On Jan. 31, 2002, the HHS secretary sent letters to state governors announcing the immediate release to the states of $207.9 million, representing the first 20 percent of nearly $1.1 billion the DOD Act sets aside for the states.

In total, the DOD Act contains approximately $2.9 billion to counter bioterrorism, including:

- $865 million for the CDC for improving state and local capacity to respond to bioterrorism;
- $135 million for grants to improve hospital capacity to respond to bioterrorism;
- $100 million for upgrading capacity at the CDC, including research (up to $10 million of which shall be for the tracking and control of biological pathogens);
- $85 million for the National Institute of Allergy and Infectious Diseases (NIAID) for bioterrorism-related research and development and other related needs;
- $70 million for the NIAID for the construction of a biosafety laboratory and related infrastructure costs;
- $593 million for the National Pharmaceutical Stockpile;
- $512 million for the purchase of smallpox vaccine;
- $71 million for improving laboratory security at the National Institutes of Health and the CDC;
- $7.5 million for environmental hazard control activities conducted by the CDC;
- $10 million for the Substance Abuse and Mental Health Services Administration; and
- $55.8 million for bioterrorism preparedness and disaster response activities in the Office of the HHS secretary.

At the discretion of the HHS secretary, these amounts may be transferred between categories subject to normal reprogramming procedures. The DOD Act also appropriates $140 million to provide grants to public entities, not-for-profit entities, and Medicare- and Medicaid-enrolled suppliers and institutional providers to reimburse them for health care related expenses or lost revenues directly attributable to the public health emergency resulting from the Sept. 11th terrorist acts. Those funds are available only when none of the costs have been reimbursed, or are eligible for reimbursement, from other sources.

In addition, on June 6, 2002, the HHS secretary announced the approval of the states' bioterrorism preparedness plan and the release of the remaining funds the federal government has allocated for preparation for bioterrorism for 2002.[60] The money will go to the 50 states (as well as the District of Columbia), eight territories, and Chicago, Los Angeles and New York City, and will be used to further develop bioterrorism readiness plans, upgrade disease recognition abilities, improve hospital readiness and enhance communications between governments and health care providers.

President Bush's fiscal year 2003 budget proposal allocates approximately $37 billion for homeland security, including $3.5 billion for first responders and $5.9 billion for the war on bioterrorism.[61] While the fiscal 2003 budget process is still young, the proposal nevertheless represents a substantial increase over the fiscal 2002 funding allocations for these areas. If this trend continues and a budget resembling President Bush's proposed budget is enacted, the federal government will appropriate significant funds for which health care providers may be eligible.

[58] H.R. 3448, § 201.

[59] P.L. No. 107-117, 115 Stat. 2229 (Jan. 10, 2002).

[60] The funding allocation can be found at http://www.hhs.gov/ophp/funding/ (last visited June 28, 2002). *See also* http://www.hhs.gov/news/press/2002pres/20020606c.html (last visited June 28, 2002).

[61] A copy of President Bush's fiscal 2003 budget proposal is available online at http://www.c-span.org/fy2003/budgetdocs/budget.pdf (last visited June 28, 2002).

 COPYRIGHT © 2002 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C. HLR ISSN 1064-2137

## Conclusion

The challenges facing health care providers in the wake of the Sept. 11th terrorist attacks are significant. With respect to health information privacy and confidentiality, the Privacy Rule contemplates and, subject to a number of varying but relatively limited requirements, permits disclosures of PHI when responding to, or attempting to prevent, terrorist activities. Accordingly, looking forward to the April 14, 2003, compliance date for the Privacy Rule, providers should incorporate the standards set forth in the Privacy Rule as they revise and update their disaster preparedness plans and otherwise consider how to respond to the threat of bioterrorism.

In addition, in light of the USA PATRIOT Act, the Bioterrorism Act, and state bioterrorism-related legislation, health care providers should increase their vigilance regarding their inventory of biological agents and toxins, and those individuals who have access to such materials.

Finally, health care providers should work aggressively with their industry consortia and state governments to seek and obtain the funding necessary to cover the significant costs of these efforts, some of which will be available from newly created sources.