THE STATE OF NEW HAMPSHIRE

MERRIMACK, SS SUPERIOR COURT

Docket No. 217-2012-CV-00617

EXETER HOSPITAL, INC.

v.

DR. SHARON ALROY-PREIS, ET AL.

MEMORANDUM OF LAW IN SUPPORT OF OBJECTION TO MOTION FOR PROTECTIVE ORDER

Defendants, Dr. Sharon Alroy-Preis, Dr. Jose Montero and New Hampshire Department of Health and Human Services (collectively hereafter "Public Health" or the "Department"), by and through their counsel, the Office of the Attorney General, submit the following Memorandum of Law in Support of Public Health's Objection to Exeter Hospital's Motion for Protective Order.

I. Introduction and Background

On May 15, 2012, Exeter Hospital reported to Public Health a cluster of recently diagnosed cases of hepatitis C at Exeter Hospital. *See* Affidavit of Dr. Sharon Alroy-Preis ("Alroy-Preis Aff.") (Respondents' Exhibit 9) ¶ 3; Respondent's Exhibit 1. The report of the cluster to Public Health was required under New Hampshire law and included disclosure of protected health information ("PHI"). *See* RSA 141-C:7 and :8; N.H. Admin. R. He-P 301.02(a)(1)(z) (requiring report of "[a]ny suspect outbreak, cluster of illness, or unusual occurrence of disease that may pose a threat to the public's health"); N.H. Admin. R. He-P 802.21(b)(5) (requiring hospitals to establish documentation procedures for "[r]eporting of infection and communicable diseases as *required by He-P 301*" (emphasis added)); Respondents' Exhibit 1(New Hampshire Communicable Disease Report Form); Respondents'

Exhibit 2 (Exeter Hospital Notice of Health Information Practices) ("We *will* disclose personal health information when required by federal, state and local law." (emphasis added)).

Hepatitis C is a viral infection that can cause life-threatening liver disease. *See* Alroy-Preis Aff. ¶ 4. In cases of active infection, the virus can be found in the infected person's blood. *See id.* Most people who develop hepatitis C do not have symptoms at all. *See id.* The virus infects a person's liver causing inflammation that can result in damage to the liver tissue. *See id.* While some people will never have complications from chronic hepatitis C infection, in others the infection may result in liver cirrhosis, liver failure, liver cancer or death. *See id.* Some people with chronic infection can be treated with effective antiviral medications. *See id.*

As a result of Exeter Hospital's report, Public Health began an investigation to determine whether the cluster is truly an outbreak. *See id.* ¶ 5; *see also* RSA 141-C:9. Once Public Health gathered information sufficient to conclude the reported cases are related, the goals of the investigation have been: (1) to stop transmission of the infection by establishing, and disrupting, the mode of transmission; and (2) to determine the scope of the outbreak by identifying all those impacted and to allow linkage to appropriate care. *See id.* In its investigation, Public Health has been utilizing various methods including, but not limited to, interviewing hospital employees, reviewing hospital policies and procedures and reviewing patient medical records. *See id.* ¶ 6.

Early in the investigation when Public Health requested review of medical records, Exeter Hospital facilitated review of electronic medical records ("EMR") through the use of the Exeter Hospital Infection Preventionist's ("IP") credentials. *See id.* ¶ 9; Affidavit of Elizabeth R. Daly (Daly Aff.) (Respondents' Exhibit 10) ¶ 6, 16; *see also* N.H. Admin. R. He-P 802.21(k) (requiring hospital administrator to appoint infection control officer). On nine occasions over a period of two months, when the Public Health investigation team (usually 2-3 persons) arrived at

Exeter Hospital, the IP identified vacant workstations for the team to sit at and logged into the computers using the IP's credentials to provide the investigation team access to the EMR database. *See* Daly Aff. ¶ 6. The secondary IP logged team members in when the primary IP was not available. *See id.* The IP left the room while the team completed the EMR reviews but remained in the vicinity to answer questions or to resolve access problems. *See id.* Following this process, the Public Health team completed record reviews on May 31, 2012, June 13, 14 and 28, and July 3, 11, 16, and 26. *See* Daly Aff. ¶¶ 8, 16. During the time that this process was used, Exeter Hospital did not demand identification of the specific records or the portions of those records to be reviewed prior to making the records available to Public Health employees. *See* Alroy-Preis Aff. ¶9; Daly Aff. ¶¶ 5-6. Rather, Exeter Hospital provided open access upon being informed that the review was in furtherance of the hepatitis C outbreak surveillance and investigation.[1] *See id.*

Public Health has conducted or requested medical record reviews for any patient suspected to be related to the Exeter Hospital hepatitis C investigation to fulfill the purposes of: (1) defining the extent of the outbreak, (2) identifying and recommending testing for exposed persons enabling infected patients to seek follow up treatment, (3) identifying the source of the outbreak, (4) identifying risk factors associated with the outbreak, and (5) protecting the public and controlling the outbreak to prevent additional infections. *See* Daly Aff. ¶¶ 11-15. Based upon information gained in the investigation, the types of patients whose medical record reviews further the purposes of the investigation include Exeter Hospital patients who: were exposed and tested positive for hepatitis C virus, were exposed and died, were exposed and not tested for

[1] To facilitate communication with Exeter Hospital regarding the investigation while maintaining security, Public Health Services implemented a secure FTP exchange server. *See* Alroy-Preis Aff. ¶ 8. Public Health Services' requests containing confidential information have been uploaded on an exchange server to be accessed securely by Exeter Hospital. *See id.*

hepatitis C virus, died with hepatitis, were not known to be exposed but were diagnosed with hepatitis C at Exeter Hospital's laboratory, were seen in the emergency department for hepatitis, may have been exposed based upon epidemiological information, or are Exeter Hospital employees that are hepatitis C positive or have unknown hepatitis C status. *See id.*

The main source of information used for accessing information has been Exeter Hospital's general EMR database (called MEDITECH). *See id.* ¶ 13. Public Health has used the MEDITECH database to collect case information including patient demographics, underlying medical conditions, laboratory testing information, procedure notes, nursing notes, medications (discontinued and current), hepatitis C risk factors, previous hepatitis C diagnoses, and information on the types of exposures (visits, admissions, surgical and diagnostic procedures, etc.) that the patient had at Exeter Hospital. *See id.* In addition, there were sources of patient information stored separately from the EMR that the Department did not have access to electronically and therefore made requests for hard copies. *See id.* These sources include MacLab, which is an independent electronic documentation system for the cardiac catheterization lab, Live Patient Activity system, and PYXIS, which contains pharmacy records from the automated medication dispensing system. *See id.*

To ensure that the Department acquired and retained only the minimum amount of information needed for the investigation, several software tools were developed to collect information from the EMR. *See id.* ¶ 14; *see also* RSA 141-C:10, IV. Those tools collected only the targeted information. *See* Daly Aff. ¶ 14. For example, the Death Medical Record Extraction Tool was only used for exposed patients that died and other Exeter Hospital patients that died from a hepatitis-related cause. *See id.* The information that was selectively collected from those records included: demographics, death information, possible hepatitis C-related

symptoms, past history of hepatitis C, hepatitis C test results, liver enzyme function test results, and hepatitis C risk factor information. In addition to manual collection tools, the Department through the use of EpiInfo (a software program developed by the Centers for Disease Control and Prevention ("CDC") designed to extract information from EMR systems for disease surveillance and investigation use) extracted information into a database that contained 549 variables. *See id.* In brief, this database collects demographics, past history of hepatitis C, hepatitis C test results, liver enzyme function test results, hepatitis C risk factor information, underlying medical conditions, medications, and information on Exeter Hospital exposures (emergency department visits, hospitalizations, procedures) since January 1, 2009 and related controlled substance drug administration associated with these exposures. *See id.*

In early August, Public Health employees involved in the records reviews signed an "End User Security Agreement – Outside Individual Access" in connection with Exeter Hospital's issuance of individualized login names and passwords that would provide access to EMR. *See* Daly Aff. ¶ 9; Respondent's Exhibit 3; Alroy-Preis Aff. ¶ 13. Use of the individualized logins allows Exeter Hospital to better maintain an accurate audit trail of the records accessed by each user.[2] *See* Alroy-Preis Aff. ¶ 13. Each Public Health investigator involved in the record review process has signed the End User Security Agreement provided by Exeter Hospital. *See* Daly Aff. ¶ 9; Respondent's Exhibit 3; Alroy-Preis Aff. ¶ 13. The purpose of the agreement "is to define standards and procedures for end users who have legitimate need to access data and systems from a device connected to Exeter Health Resources' (EHR) network." *See* Respondent's Exhibit 3. "The overriding goal of th[e] agreement is to protect the confidentiality, integrity and

[2] Because investigators were previously logged in under an Exeter Hospital employee's name, in order to keep an accurate accounting of the investigators' reviews under the prior process, the IP would have had to keep a separate log specifying the name of the Public Health investigator. With individualized user names and passwords maintaining a separate log is not necessary.

availability of the data and systems that reside[] within EHR's technology infrastructure and to secure protected health information (PHI) and personally identifiable information (PII) data in storage, in transit, and in use." *See id.* Each signer agreed that "[i]t is the responsibility of anyone who uses a device to access EHR data and resources, to adhere to and comply with all EHR privacy/security policies and applicable laws." *See id.* Each signer further agreed that she will be "accountable for all work done under [her] code" and "will NOT intentionally attempt to access any information not authorized for [her] use via [her] PASSWORD." *See id.* By providing user name and password for each Public Health investigator, Exeter Hospital can audit each investigator's access to records. *See* Alroy-Preis Aff. ¶ 13.

As a result of its early investigation, Public Health determined that the cases reported by Exeter Hospital (3 patients and 1 healthcare worker) shared a common link: being in the hospital cardiac catheterization laboratory (CCL) or its recovery room (RR). *See id.* ¶ 10. Further testing by Public Health revealed that all four had identical sequences of the virus, proving a common source of infection. *See id.* Based on the epidemiological investigation (which included medical record review), Public Health determined that the most likely mechanism of transmission is narcotic diversion by the HCV positive healthcare worker. *See id.* In addition to medical record reviews, hospital employee interviews and other investigative methods, Public Health collected and tested blood specimens from 1,144 persons of the 1,293 (who were recommended by Public Health for testing because they were either CCL/RR patients (1066) or employees (78)). *See id.* ¶ 11. As a result of this testing, Public Health has already identified 33 people with an active HCV strain that matches the outbreak strain and 28 additional patients who have evidence of a past HCV infection that has cleared. *See id.* Because it is not possible to conduct molecular tests (virus sequencing) for patients with cleared infections, additional epidemiological investigation

including medical record review is necessary to determine whether patients with cleared infections might have been acquired as part of this outbreak. *See id.*

This is an ongoing investigation that will require gathering additional information from Exeter Hospital, its employees and regional providers as well as state and federal agencies, including the CDC. *See id.* ¶ 12. Based on information from the ongoing investigation, Public Health discovered that the healthcare worker suspected of narcotic diversion may have also been present in the main inpatient operating room (OR) and the intensive care unit (ICU) at Exeter Hospital. *See id.* Given this new information, Public Health recommended testing for patients who received care in these areas during the time of employment of the implicated healthcare worker. *See id.* Outstanding questions remain regarding the mode of transmission and the scope of the outbreak. *See id.*

In July and August, Exeter Hospital began asking Public Health to provide information about facts learned in the investigation including the results of tests performed by Public Health. *See* Alroy-Preis Aff. ¶ 14. After Public Health told Exeter Hospital that it was prohibited from sharing such protected health information under RSA 141-C:10, Exeter Hospital began resisting Public Health's requests. *See id.* Among other things, Exeter Hospital refused to allow interviews of staff unless such interviews were monitored by an Exeter Hospital representative and it refused to provide access to patient medical records unless Public Health first provided evidence sufficient for Exeter Hospital to conclude that the information requested was definitely linked to the already established cluster. *See id.* In other words, Exeter Hospital obstructed access to medical records except for those of patients within the established cluster. To buttress its efforts to deny future access, Exeter Hospital declared the records privileged and not subject to disclosure under state and federal law. *See* Alroy-Preis Aff. ¶ 14-16.

On August 21, 2012, Exeter Hospital sent a letter explaining its newly found claim of privilege. *See* Respondent's Exhibit 3. On August 24, 2012, Public Health uploaded a document onto the FTP server providing written notification to Exeter Hospital that a Public Health investigator would be making a site visit to Exeter Hospital to review the records of a specific patient. *See* Petitioner's Exhibit B; Alroy-Preis Aff. ¶ 14. In the notice, Exeter Hospital was informed that the purpose of the review was for "[o]utstanding questions regarding possible exposure to HCV at the hospital" and that "[t]his record review falls within the purview of the HCV outbreak investigation and [Public Health] will review no more than the necessary information." *See id.* When the Public Health investigator arrived at Exeter Hospital, she was met by outside counsel for Exeter Hospital who told her that unless she provided additional information about her review including specific information as to "why this patient is connected to the DPH investigation" she would not be allowed access. *See* Petitioner's Exhibit D.

II. State law provides Public Health with broad authority to investigate occurrences of communicable diseases including requiring disclosure of otherwise protected health information.

RSA 141-C:1 declares that it is the policy of the State of New Hampshire that "communicable diseases be prevented, and that such occurrences be identified, controlled, and, when possible, eradicated at the earliest possible time by application of appropriate public health measures and medical practices." In furtherance of this policy RSA chapter 141-C provides the Commissioner of the Department of Health and Human Services with broad authority to: (1) require reporting of communicable disease, RSA 141-C:7, (2) investigate incidents of communicable disease including requiring individuals to submit to physical examination and to submit specimens of body secretions, excretions, body fluids, and discharges for examination and require reporting officials, their patients, and other persons affected by or having information

pertaining to the communicable disease to provide information and periodic reports and to respond to surveys, RSA 141-C:9, (3) order isolation or quarantine for persons or commodities that are cases or suspected cases of communicable diseases, RSA 141-C:11, (4) require persons infected with a communicable disease to submit to treatment, RSA 141-C:15, (5) compel (with written approval of the governor) evacuation and decontamination of any building accessible to the public and order destruction of property, RSA 141-C:16-a, (6) order (with written approval of the governor) cancellation of public gatherings and events, RSA 141-C:16-b, and (7) require parents to have their children immunized against certain diseases, RSA 141-C:20-a. *See* RSA 141-C:4.

The hepatitis C outbreak at Exeter Hospital implicates the provisions of RSA chapter 141-C that require healthcare providers to report an incidence of communicable disease and to provide additional information including protected health information to Public Health authorities charged with conducting an investigation. Pursuant to RSA 141-C:8, the Commissioner has "compile[d] a list of reportable communicable diseases necessary to protect the citizenry." *See* N.H. Admin. R. He-P 301.02. In addition to each incidence of specified diseases, healthcare providers are required to report "[a]ny suspect outbreak, cluster of illness, or unusual occurrence of disease that may pose a threat to the public's health." N.H. Admin. R. He-P 301.02(a)(1)(z). To assure compliance with Administrative Rule He-P 301, Exeter Hospital, as a hospital licensed under RSA chapter 151, is required to appoint an infection control officer who shall "[r]eport to the director of public health services all diseases for which reporting is required under RSA 141-C." N.H. Admin. R. He-P 802.21(k). Consistent with this obligation and its practices, Exeter Hospital's reporting official, Jackie Dockham, reported the suspected

hepatitis C cluster of cases to Public Health on May 15, 2012. *See* Respondent's Exhibits 1 and 2; *see* N.H. Admin. R. He-P 301.03.

RSA 141-C:9, I, provides that the "commissioner or designee may investigate incidents of communicable diseases" and that "[s]uch investigations shall include, but not be limited to, *requiring* additional information and periodic reports from the reporting official, interviews with the reporting officials, their patients, and other persons affected by or having information pertaining to the communicable disease, surveys of such individuals, inspections of buildings and conveyances and their contents, and laboratory analysis of samples collected during the course of such inspections." (Emphasis added.) Pursuant to Administrative Rule He-P 301.07(b)(5), the Department's investigation *shall* include "[r]eview of individual case medical records, business records, reports and x-rays of cases, *suspect cases and contacts in a disease incident.*" (Emphasis added.) Hence, in investigating the hepatitis C outbreak at Exeter Hospital, the Department may require Exeter Hospital to provide access to medical records of suspect cases *and contacts*. As a licensed facility under RSA chapter 151, Exeter Hospital is required to make patient records available to the Department for review. *See* N.H. Admin. R. He-P 802.20. Furthermore, Exeter Hospital provides notice to its patients that it discloses personal health information as required by state law and that such disclosures do not require patient authorization. *See* Respondents' Exhibit 2 (http://www.exeterhospital.com/gedownload!/507%20Notice%20of%20Health%20Information%20Practices%2003-2011.pdf?item_id=169198033&version_id=169198034).

Although RSA 141-C:9 generally states that "[t]he commissioner shall adopt such rules as are necessary to carry out investigations with due regard for the rights of person and property," RSA 141-C:10, III specifically provides that "[t]he physician-patient privilege shall

not apply to information required to be reported or provided to the commissioner under this chapter." RSA 329:26 correspondingly states that the physician-patient privilege applies "except as otherwise provided by law." Because RSA 141-C:10, III specifically states that RSA 329:26 does not apply, RSA 329:26 cannot be used by Exeter Hospital as a shield against complying with its obligation to make patient records available for the Department's review.[3]

In removing the physician-patient privilege to ensure that the Department can perform its duties, the legislature did not leave PHI disclosed in the context of an investigation without protection. Rather, in recognition of the Department's authority to require access to information, the Department may "acquire and retain only the minimum amount of information, specimens, and samples necessary to carry out its obligations." RSA 141-C:10, IV. Moreover, the Department's authority to re-disclose PHI is strictly limited. RSA 141-C:10, I states:

> Any protected health information provided to or acquired by the department under this chapter shall be released only with the informed, written consent of the individual or to those authorized persons having a legitimate need to acquire or use the information and then only so much of the information as is necessary for such person to provide care and treatment to the individual who is the subject of the protected health information, investigate the causes of disease transmission in the particular case, or control the spread of the disease among the public. Any release of information under this section without the informed, written consent of the individual shall be conditioned upon the protected health information remaining confidential.

Thus, the Department may *acquire* and *disclose* PHI only for the purposes of the investigation, which, among other things, includes identifying suspect cases and allowing linkage to appropriate care. And, any release of information by Public Health under RSA 141-C:10, 1, must be conditioned upon the protected health information remaining confidential.

---

[3] *In re Search Warrant (Med. Records of C.T.)*, 160 N.H. 214, 216-17 (2010) has no application here because the statute at issue in that case did not contain an express exception to RSA 329:26.

The methods employed by the Department in this investigation fully comply with RSA chapter 141-C. In their review of medical records, Public Health investigators have acquired the minimum amount of information necessary for purposes of the investigation. An investigation by its very nature requires reviewing relatively broad range of records to determine whether relevant information is contained within them. As explained above, the methods by Public Health are calculated to ascertain information to further the purposes of the investigation. The information Public Health has acquired is the minimum necessary to (1) define the extent of the outbreak, (2) identify and recommend testing for exposed persons, (3) identify the source of the outbreak, (4) identify risk factors associated with the outbreak, and (5) protect the public and control the outbreak to prevent additional infections. Some information gathered by Public Health may exclude potential sources; other information may provide leads that must be followed before a potential source is identified or excluded. As with any investigation, to maintain the integrity of the investigation Public Health is limited in the amount of information that it may share with Exeter Hospital, the facility where the infection was spread. Further, Public Health is limited by RSA 141-C:10 to disclosing to Exeter Hospital and others only the minimum amount of information necessary for the purposes of the investigation. Providing Exeter Hospital with an explanation regarding why the information is sought would jeopardize the integrity of the investigation and likely violate the statute because it would often require disclosure of more information than minimally necessary to identify suspect cases and allow linkage to care.

Moreover, RSA chapter 141-C does not authorize a healthcare provider such as Exeter Hospital to determine whether an investigation of a potentially life-threatening communicable disease is necessary to protect the public's health or the scope of that investigation. That

authority is squarely placed with the Commissioner. *See* RSA 141-C:4, :9. Allowing Exeter Hospital to demand conclusive proof that a medical record is definitively linked to the outbreak prior to providing access would confer a gate-keeping function to be served by the hospital that is absent from the statute. *Cf. Ohio Legal Rights Serv. v. Buckeye Ranch, Inc.*, 365 F. Supp. 2d 877, 885 (S.D. Ohio 2005) (concluding where statute provides access to otherwise protected records children with mental illness, allowing institution to demand conclusive individualized showing of mental illness before permitting access would reserve gate-keeping function to institution contrary to specific terms and general purpose of statute).

III. HIPAA does not limit Public Health's authority to require access to protected health information for the purposes of a public health investigation.

In enacting the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Congress sought to "improve the Medicare program . . ., the medicaid program . . ., and the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information." Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 261 (1996). In recognition of Public Health's need for access to fulfill its duties, Congress specifically provided:

> PUBLIC HEALTH. -- Nothing in [HIPAA] shall be construed to invalidate or limit the authority, power or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention.

42 U.S.C. § 1320d-7(b). Consistent with this declaration, the Secretary, promulgated rules adopting Standards for Privacy of Individually Identifiable Health Information, which allow for disclosure of PHI to public health authorities. *See generally* 45 C.F.R. Parts 160 and 164 (65 Fed. Reg. 82,462 *et seq.* (2000)).

"The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information to carry out their public health mission." *See* U.S. Department of Health and Human Services, Office for Civil Rights Disclosures for Public Health Activities, http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/publichealth/publichealth.pdf, Respondents' Exhibit 4. The General Administrative Requirements provide that "[a] standard, requirement, or implementation specification adopted under [HIPAA] that is contrary to a provision of State law preempts the provision of State law." 45 C.F.R. § 160.203. The general rule, however, does not apply if "[t]he provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention." 45 C.F.R. § 160.203(c).

Consistent with HIPAA's recognition for access by public health officials as determined by state and federal law, 45 C.F.R. § 164:512(a)(1) regarding uses and disclosures of protected health information provides that a covered entity such as Exeter Hospital may disclose PHI without written authorization of the individual or the opportunity for the individual to agree or object "to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law." *See also* Respondents' Exhibit 4. Hence, the HIPAA privacy rule "permits covered entities to use or disclose protected health information when they are required by law to do so," 65 Fed. Reg. at 82666, and it is intended "to preserve access to information considered important enough by state or federal authorities to require its disclosure by law, *id.* at 82667.

> The importance of these required uses or disclosures is evidenced by the legislative or other public process necessary for the government to create a legally binding obligation on a covered entity. Furthermore, such required uses and disclosures arise in a myriad of other areas of law, ranging from topics addressing national security (uses and disclosures to obtain security clearance), to public health (reporting of communicable diseases), to law enforcement (disclosures of gunshot wounds). Required uses and disclosures also may address broad national concerns or particular regional or state concerns. It is not possible, or appropriate, for HHS to reassess the legitimacy of or the need for each of these mandates in each of their specialized contexts. In some cases where particular concerns have been raised by legal mandates in other laws, [HHS] allow[s] disclosure as required by law, and [it] establish[es] additional requirements to protect privacy (for example, information the individual as required in § 164.512(c)) when covered entities make a legally mandated disclosure.

Id. In sum, "[t]he rule's approach is simply intended to avoid any obstruction to the health plan or covered health care provider's ability to comply with its existing legal obligations." *Id.* at 82668.

New Hampshire law authorizes the Department to investigate incidents of communicable diseases and pursuant to such investigations *to require* health care providers such as Exeter Hospital to provide review of individual patient records. *See* RSA 141-C:9, I; N.H. Admin. R. He-P 301.07(b)(5); He-P 802.20. The protective order Exeter Hospital seeks would be contrary to the express recognition in HIPAA of the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information to carry out their public health mission and the intention that HIPAA not stand in the way of such activities whether granted under state or federal law.

IV. The minimum necessary rule does not apply to disclosures of PHI in the context of a communicable disease investigation conducted pursuant to RSA chapter 141-C.

The minimum necessary requirement does not apply to "disclosures that are required by law, as described by § 164.512(a)." 45 C.F.R. § 164.502(b)(2)(v); 65 Fed. Reg. 82462, 82498 (2000) (covered entities permitted to disclose for public policy purposes determined by state law

in compliance with § 164.512 may disclose without any condition); *see Abbott v. Tex. Dep't of Mental Health & Mental Retardation*, 212 S.W.3d 648, 660 (Tex. App. Ct. 2006). As set forth above, New Hampshire law authorizes the Department to investigate incidents of communicable diseases and pursuant to such investigations *to require* health care providers such as Exeter Hospital to provide review of individual patient records. *See* RSA 141-C:9, I; N.H. Admin. R. He-P 301.07(b)(5); He-P 802.20.

The Privacy Rule provision for uses and disclosures for which an authorization or opportunity to agree is not required contains two provisions, one for disclosures that are required by law, 45 C.F.R. § 164.512(a), and another for disclosures that are not required by law but authorized by law, 45 C.F.R. § 164.512(b). *See* Salvatore Lucido and Denise Koo, HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services, p. 8 (April 11, 2003) (http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm) ("Guidance from CDC and US DHHS"), Respondents' Exhibit 5.

> *Required by law* means a mandate contained in a law that compels an entity to make a use or disclosure of protected health information that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or trial inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

45 C.F.R. § 164.103 (emphasis in original). Because Exeter Hospital is required by State statute and regulations promulgated thereto to provide access to medical records in the context of a communicable disease investigation, RSA 141-C:9, I, N.H. Admin. R. He-P 301.07(b)(5), He-P

802.20, HIPAA allows Exeter Hospital to disclose in compliance with the state law without further condition. *See Buckeye Ranch, Inc.*, 365 F. Supp. 2d at 890; 45 C.F.R. § 164.512(a) *see also* KATHY BAKICH AND JOANNE HUSTEAD, EMPLOYER'S GUIDE TO HIPAA PRIVACY REQUIREMENTS, ¶ 311, p. 55 (2010) (minimum necessary standard does not apply to uses or disclosures required by other laws).

The minimum necessary rule comes into play only where Public Health collects information that is authorized by law but not required by law. By way of example, the Department is generally authorized to collect health information pursuant to RSA 125:9. That statute authorizes the Department to "take cognizance of the interests of health and life among the people," RSA 125:9, I, and to generally "[m]ake investigations and inquiries concerning the causes of epidemics and other diseases, the sources of morbidity and mortality, and the effects of localities, employments, conditions, circumstances, and the environment on the public health," RSA 125:9, II. The minimum necessary rule *might* apply where Public Health is collecting and receiving information pursuant to this general grant of authority under RSA 125:9 and no other provision of law requiring disclosure to Public Health exists. *See* 45 C.F.R. §164.512(b)(1)(i); Guidance from CDC and US DHHS, Exhibit 5, p. 8 ("DHHS interpreted the phrase 'authorized by law' to mean that the a legal basis exists for the activity."). Because New Hampshire not only authorizes but requires disclosure of information for incidents of communicable diseases investigated under RSA 141-C:9, the minimum necessary rule does not apply.

V. Even if the minimum necessary rule were to apply, Exeter Hospital would be able to rely on Public Health's representation that the information requested is the minimum necessary for the stated purpose of resolving outstanding questions regarding possible exposure to HCV at the hospital.

The Privacy Rule, 45 C.F.R. § 164.514(d)(3)(iii), provides: "Any covered entity may rely, if such reliance is reasonable under this circumstances, on a requested disclosure as the

minimum necessary for the stated purpose when: (A) Making disclosures to public officials under § 164.512, if the public official represents that the information is the minimum necessary for the stated purpose."[4] Exeter Hospital concedes it knows of the general legal and factual basis for the investigation of the hepatitis C outbreak at Exeter Hospital and in fact provided Public Health access on at least 11 occasions. Public Health has represented to Exeter Hospital that the record review requested is the minimum necessary for resolving the outstanding questions regarding possible exposure to HCV at the hospital. It would be contrary to the purpose of the communicable disease statute and the express authority to investigate incidents of communicable disease to allow Exeter Hospital to deny Public Health access to the records of patients, who Public Health believes may have been affected by an outbreak of a potentially life-threatening communicable disease, unless Public Health first provides Exeter Hospital with a brief explanation of the factual basis for each specific request.[5] Further, the minimum necessary rule under HIPAA is not intended to create such a gate-keeping function. *See* 85 Fed. Reg. 82530 ("A covered entity is not required to second guess the scope or purpose of the request, or take action to resist the request because they believe that it is over broad.").

The minimum necessary requirements are met where the disclosure is made within the scope of the permitted authorization. Here, in the context of an investigation where at least 31 patients have already been identified as being infected while receiving treatment at Exeter Hospital, it is appropriate for the hospital, presented with a relatively broad request, to permit

---

[4] The minimum necessary requirements of 45 C.F.R. § 164.514 set forth requirements "[i]n order to comply with 164.502(b) and this section . . . ." Because 164.502(b) applies only to disclosures authorized by law but not required by law, this section does not apply.

[5] While Public Health has an interest in determining the full extent of the outbreak, identifying not only confirmed cases but also probable and suspect cases, Exeter Hospital does not necessarily share that interest especially in view of the potential for liability in causing the outbreak.

access to a relatively large amount of information in order to identify the relevant information. Thus, even if the minimum necessary rule were to apply, it would allow for review of a relatively large amount of information to determine the full scope of the infection.

VI. HIPAA's audit requirements and EMR system do not require prior disclosure of the records to be reviewed.

HIPAA requires covered entities such as Exeter Hospital to provide an accounting upon request to an individual of disclosures of PHI made in the prior to the date of the request. *See* 45 C.F.R. § 164.528(a). Nothing in HIPAA relative to accounting allows a covered entity to dictate the scope of a communicable disease investigation. For each disclosure, the accounting must include: (1) the date of the disclosure; (2) the name of the entity or person who received the protected health information and, if known, the address of such entity or person; (3) a brief description of the PHI disclosed; and (4) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure or, in lieu of such statement, a copy of the written request for a disclosure under 164.512, if any. The rule does not require an accounting of the particular details of the information actually viewed by Public Health. *See* Respondents' Exhibit 6 (Health Information Privacy www.hhs.gov/ocr/privacy/hipaa/faq/public_health_uses_and_disclosures/465.html) (describing appropriate accounting of disclosures that involve public health authority access to an entire universe of records). Rather, "[w]here, as with many public health disclosures, access to an entire universe of records is involved, tracking disclosures can be accomplished without the need for documentation in each record." *See id.* For example, if on October 1, 2012, Exeter Hospital began providing Public Health with access to the medical charts of all patients treated in its emergency department from October 1, 2010 to June 30, 2012 to identify suspect cases or for some other purpose related to the investigation of the outbreak and to extract relevant

information required for that purpose, it would be sufficient for the accounting to include the following:

- the identity, and address, if known, of the public health authority;
- a statement that the public health authority had access to medical charts for patients treated in the emergency department;
- the date (or approximate range of dates when the individual's record was subject to access; and
- a statement of the purpose of the access (*e.g.*, investigation of hepatitis C outbreak).

See Respondents' Exhibit 6. In response to a request for accounting as set forth in the example above, Exeter Hospital could provide the same basic statement in response to a request by any individual who was seen in the emergency department of the hospital between October 1, 2010 and June 30, 2012 and be fully in compliance with its duty to account for such uses and disclosures to Public Health. *See id.*

Further, in the event Exeter Hospital wanted to provide its patients with a more detailed accounting, it is likely that the EMR database used by Exeter Hospital could provide more detailed information. Exeter Hospital maintains a general EMR database on a system called MEDITECH. To comply with HIPAA technical safeguards, Exeter Hospital must implement controls including (1) assigning a unique name or number for identifying and tracking user identity, and (2) implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. *See* 45 C.F.R. § 164.312(a)(2). Many EMR database systems have such security features built in. *See* U.S. Department of Health and Human Services, How Do I Ensure Security in Our System? (http://www.hrsa.gov/healthit/toolbox/HIVAIDSCaretoolbox/SecurityAndPrivacyIssues/howdoiensuresec.html), Respondents' Exhibit 7. MEDITECH claims that its system "incorporates

multi-tiered access control features that provide protection across all levels and types of access, as well as system-wide audit trails that track the viewing and editing of data." *See* Respondents' Exhibit 8. Because MEDITECH automatically provides audit trails that track viewing of data, advance notice of the records to be reviewed would not be necessary even if Exeter Hospital chose to provide its patients with a detailed accounting of the specific records accessed.

VII. The State statutes cited by the Petitioner would not prohibit Public Health's access to records.

In a final effort to obstruct access, the Petitioner cites a laundry list of State statutes claiming that because of these statutes Public Health access is generally prohibited from accessing Exeter Hospital's medical records. Some of the statutes expressly allow access where provided by other law. *See* RSA 151:21, X; RSA 332-I:2, I(e). Because access is expressly allowed under RSA 141-C:9, these statutes allow Public Health access. The HIV testing statute expressly requires disclosure to Public Health. *See* RSA 141-F:7, I(b). The statutes that do not provide an exception for access otherwise provided by law do require heightened security. *See, e.g.*, RSA 141-F:8, II. Due to these security requirements, there is no apparent reason that Exeter Hospital would have records subject to those statutes in its EMR database open to review to any person with general access to clinical records. *See* Exhibit 8 (MEDITECH Electronic Health Record Functionality Brief) ("Confidential patient and VIP flags may be used to prevent users from accessing the records of patients located within confidential locations or who have been assigned a confidential status."). Maintaining such highly sensitive records in its general EMR database would likely subject those records to disclosure to *any user* of the database and therefore violate those statutes' confidentiality provisions. Moreover, it is not apparent that Exeter Hospital maintains any such records – Exeter Hospital has not asserted in its pleadings that it provides genetic testing, *see* RSA 141-H:2, operates a federally-funded or certified drug or

alcohol rehabilitation facility, *see* RSA 172:8-a, operates a rape crisis center or a domestic violence center, *see* RSA 173-C:2, or operates New Hampshire Hospital or one of its designated receiving facilities, *see* RSA 135-C:19-a. Finally, Public Health investigators have already agreed "to adhere to and comply with all EHR privacy/security policies and applicable laws." *See* Respondents' Exhibit 3. Thus, a protective order is not necessary to obtain compliance with such laws.

In sum, Exeter Hospital's request for a protective order should be denied because rather than limiting access, state and federal laws expressly provide Public Health access to patient records. State law expressly requires Exeter Hospital to provide information to the Public Health pursuant to an investigation of a communicable disease, RSA 141-C:9, I, and abrogates the physician-patient privilege for the purpose of providing such information, RSA 141-C:10, III. Further, Congress has declared that "[n]othing in [HIPAA] shall be construed to invalidate or limit the authority, power or procedures established under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention," 42 U.S.C. § 1320d-7(b). Thus, the HIPAA and regulations are intended to avoid any obstruction to Exeter Hospital's ability to comply with its existing legal obligations under State law.

DR. SHARON ALROY-PREIS, DR. JOSE MONTERO, AND THE STATE OF NEW HAMPSHIRE DEPARTMENT OF HEALTH AND HUMAN SERVICES

By their attorney,

MICHAEL A DELANEY
ATTORNEY GENERAL

Date: October 2, 2012 By: _____

Jeanne P. Herrick, Bar No. 13817
Attorney
Anne M. Edwards, Bar No. 6826
Associate Attorney General
New Hampshire Attorney General's Office
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3650
E-mail: jeanne.herrick@doj.nh.gov
anne.edwards@doj.nh.gov

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing memorandum of law has been mailed to:

W. Scott O'Connell, Esquire
Gordon J. MacDonald, Esquire
Anthony J. Galdieri, Esquire
Nixon Peabody, LLP
900 Elm Street, 14th Floor
Manchester, NH 03101

Date: October 2, 2012 _____
Jeanne P. Herrick, Bar No. 13817

803426

EXHIBIT 1

New Hampshire Communicable Disease Report Form 2011

DISEASE: Hep C

Patient Name _____ (Last) _____ (First) _____ (M.I.)

Date of Birth _____ Age 82 ☑ Male ☐ Female

Address _____

City/Town _____ State _____ Zip _____

Home/Cell Phone _____ Work Phone _____

Occupation/Employment _____

Race
- ☐ White
- ☑ Black
- ☐ Asian
- ☐ Pacific Islander
- ☐ Native Am./Alaskan Native
- ☐ Other
- ☐ Unknown

Ethnicity
- ☐ Hispanic
- ☑ Not Hispanic
- ☐ Unknown

Miscellaneous Information *(check all that apply)*
- ☐ Pregnant # of weeks _____
- ☐ Healthcare Worker
- ☐ Nursing Home Resident / Worker
- ☐ Day Care Child / Worker
- ☐ Food Service Worker
- ☐ Deceased
- ☑ Hospitalized (if yes, where?) 5/3-5/7 5/13 → present

Card Letter 1/30/12

Symptom Onset Date _____
Diagnosis Date _____
Date of Test _____
Type of Test _____
TB (PPD) mm _____
Chest X-ray Date: _____
Chest X-ray: ☐ Abnormal ☐ Normal

Specimen Source
- ☐ Blood
- ☐ Cervix
- ☐ Stool
- ☐ Urethra
- ☐ Urine
- ☐ Rectum
- ☐ Pharynx
- ☐ Unknown
- ☐ Other *(specify)*

Treatment
Date _____
Drug _____
Dosage _____ Days _____

Patient aware of diagnosis?
- ☑ YES
- ☐ NO
- ☐ Unknown

If reporting a Vaccine Preventable Disease, please indicate if patient was previously vaccinated for this infection:
☐ NO ☐ YES Date Administered: _____

Healthcare Provider Information Date of Report _____

Reported by Jackie Dockham Phone _____

Healthcare Provider Dr Mark L.M - Maine PCP Phone _____

Name of Facility Exeter Hosp

City/Town Exeter State NH Zip 03833

Reporting a Communicable Disease
Phone: 1-603-271-4496 or 1-800-852-3345 ext. 4496
Hotline: 1-888-836-4971
After Hours Response: 1-603-271-5300
Toll Free After Hours: 1-800-852-3345 ext. 5300
Fax: 1-603-271-0545 DO NOT FAX HIV reports
Mail: NH Department of Health and Human Services
Division of Public Health Services
Bureau of Infectious Disease Control
29 Hazen Drive, Concord, NH 03301-6504

NH RSA 141-C and He-P300 mandate reporting of the listed communicable diseases by all physicians, labs, and health care providers. We request prompt reporting of suspect and confirmed cases as well as any suspect outbreaks of illness. All reports are handled under strict confidentiality standards.

Diseases with an (*) must be reported within 24 hours of diagnosis
All others must be reported within 72 hours of diagnosis

-Acquired Immune Deficiency Syndrome (AIDS)
-Anaplasmosis [*Anaplasma Phagocytophilum*]
-Anthrax [*Bacillus anthracis*]*
-Arboviral infection, including EEE & WNV*
-Babesiosis [*Babesia microti*]
-Botulism [*Clostridium botulinum*]*
-Brucellosis [*Brucella abortus*]*
-Campylobacteriosis [*Campylobacter* species]
-Chlamydial infection [*Chlamydia trachomatis*]
-Cholera [*Vibrio cholerae*]*
-Coccidioidomycosis [*Coccidioides immitis*]
-Creutzfeldt-Jakob Disease*
-Cryptosporidiosis [*Cryptosporidium parvum*]
-Cyclospora infection [*Cyclospora cayetanensis*]
-Diphtheria [*Corynebacterium diphtheriae*]*
-Ehrlichiosis [*Ehrlichia* species]
-*Escherichia coli* O157 infection and other Shiga toxin producing *E. coli*
-Giardiasis [*Giardia lamblia*]
-Gonorrhea [*Neisseria gonorrhoeae*]
-*Haemophilus influenzae*, invasive disease, sterile site*
-Hantavirus Pulmonary Syndrome [Hantavirus]*
-Hemolytic Uremic Syndrome (HUS)
-Hepatitis, viral: A*, B, E, G
-Hepatitis, viral: positive B surface antigen in a pregnant woman
-Human Immunodeficiency Virus (HIV), including perinatal expo...
-Human Immunodeficiency Virus-related CD4+ counts and all vi
-Legionellosis [*Legionella pneumophila*]
-Leprosy, Hansen's disease [*Mycobacterium leprae*]
-Listeriosis [*Listeria monocytogenes*]
-Lyme disease [*Borrelia burgdorferi*]
-Malaria [*Plasmodium* species]
-Measles [Rubeola]*
-Mumps*
-*Neisseria meningitidis*, invasive disease, sterile site*
-Pertussis [*Bordetella pertussis*]*
-Plague [*Yersinia pestis*]*
-Pneumococcal disease, invasive [*Streptococcus pneumoniae*]
-Pneumocystis pneumonia [*Pneumocystis jiroveci* formerly *carin*
-Poliomyelitis [Polio]*
-Psittacosis [*Chlamydophilia psittaci*]*
-Rabies in humans or animals*
-Rocky Mountain Spotted Fever [*Rickettsia rickettsii*]
-Rubella, including Congenital Rubella Syndrome*
-Salmonellosis [*Salmonella* species] (report *S.* Typhi* within 24 hours)
-Shigellosis [*Shigella* species]
-Streptococcus Group A/B, invasive disease [*S. pyogenes/agalactiae*]
-Syphilis, including Congenital Syphilis Syndrome [*Treponema pallidum*]
-Tetanus [*Clostridium tetani*]
-Toxic-Shock Syndrome (TSS) [streptococcal or staphylococcal]
-Trichinosis [*Trichinella spiralis*]
-Tuberculosis disease [*Mycobacterium tuberculosis*]*
-Tuberculosis infection, latent
-Tularemia [*Francisella tularensis*]*
-Typhoid fever [*Salmonella* Typhi]*
-Typhus [*Rickettsia prowazekii*]*
-Varicella*
-Vibriosis [any *Vibrio* species]*
-Vancomycin Resistant Enterococci (VRE)
-Vancomycin Resistant *Staphylococcus aureus* (VRSA)*
-Yersiniosis [*Yersinia enterocolitica*]
-Any suspect outbreak, cluster of illness, or unusual occurrence of disease that may pose a threat to the public's health must be reported within 24 hours of recognition (please call reports in by phone)*

RECEIVED
MAY 16 2012
Infectious Disease Control

SCANNED
Initials: KB
Date: 8/2/12

FAXED 6-11-2012

1-207-676-9788

Good all Health

New Hampshire Communicable Disease Report Form 2011

DISEASE: ? Hep C

Patient Name _____ (Last) _____ (First) _____ (M.I.)

Date of Birth _____ Age 74 ☑ Male ☐ Female

Address _____

City/Town _____ State _____ Zip _____

Home/Cell Phone _____ Work Phone _____

Occupation/Employment _____

Race
- ☑ White
- ☐ Black
- ☐ Asian
- ☐ Pacific Islander
- ☐ Native Am./Alaskan Native
- ☐ Other
- ☐ Unknown

Ethnicity
- ☐ Hispanic
- ☑ Not Hispanic
- ☐ Unknown

Miscellaneous Information *(check all that apply)*
- ☐ Pregnant # of weeks _____
- ☐ Healthcare Worker
- ☐ Nursing Home Resident / Worker
- ☐ Day Care Child / Worker
- ☐ Food Service Worker
- ☐ Deceased
- ☐ Hospitalized (if yes, where?)

Symptom Onset Date ? March

Diagnosis Date _____

Date of Test _____

Type of Test _____

TB (PPD) mm _____

Chest X-ray Date: _____

Chest X-ray: ☐ Abnormal ☐ Normal

Specimen Source
- ☐ Blood
- ☐ Cervix
- ☐ Stool
- ☐ Urethra
- ☐ Urine
- ☐ Rectum
- ☐ Pharynx
- ☐ Unknown
- ☐ Other *(specify)*

Treatment

Date _____

Drug _____

Dosage _____ Days _____

Patient aware of diagnosis?
- ☑ YES
- ☐ NO
- ☐ Unknown

If reporting a Vaccine Preventable Disease, please indicate if patient was previously vaccinated for this infection:

☐ NO ☐ YES Date Administered: _____

Healthcare Provider Information Date of Report 5/15/12

Reported by J. Dockham Phone 5506531

Healthcare Provider Dr Wu Phone 7782899 ext 6513

Name of Facility Exeter Hosp

City/Town Exeter State NH Zip 03833

Reporting a Communicable Disease

Phone: 1-603-271-4496 or 1-800-852-3345 ext. 4496
Hotline: 1-888-836-4971
After Hours Response: 1-603-271-5300
Toll Free After Hours: 1-800-852-3345 ext. 5300
Fax: 1-603-271-0545 DO NOT FAX HIV reports
Mail: NH Department of Health and Human Services
Division of Public Health Services
Bureau of Infectious Disease Control
29 Hazen Drive, Concord, NH 03301-6504

NH RSA 141-C and He-P300 mandate reporting of the listed communicable diseases by all physicians, labs, and health care providers. We request prompt reporting of suspect and confirmed cases as well as any suspect outbreaks of illness. All reports are handled under strict confidentiality standards.

Diseases with an (*) must be reported within 24 hours of diagnosis
All others must be reported within 72 hours of diagnosis

-Acquired Immune Deficiency Syndrome (AIDS)
-Anaplasmosis [*Anaplasma Phagocytophilum*]
-Anthrax [*Bacillus anthracis*]*
-Arboviral infection, including EEE & WN
-Babesiosis [*Babesia microti*]
-Botulism [*Clostridium botulinum*]*
-Brucellosis [*Brucella abortus*]*
-Campylobacteriosis [*Campylobacter* species]
-Chlamydial infection [*Chlamydia trachomatis*]
-Cholera [*Vibrio cholerae*]*
-Coccidioidomycosis [*Coccidioides immitis*]
-Creutzfeldt-Jakob Disease*
-Cryptosporidiosis [*Cryptosporidium parvum*]
-Cyclospora infection [*Cyclospora cayetanensis*]
-Diphtheria [*Corynebacterium diphtheriae*]*
-Ehrlichiosis [*Ehrlichia* species]
-*Escherichia coli* O157 infection and other Shiga toxin producing *E. coli*
-Giardiasis [*Giardia lamblia*]
-Gonorrhea [*Neisseria gonorrhoeae*]
-*Haemophilus influenzae*, invasive disease, sterile site*
-Hantavirus Pulmonary Syndrome [Hantavirus]*
-Hemolytic Uremic Syndrome (HUS)
-Hepatitis, viral: A*, B, E, G
-Hepatitis, viral: positive B surface antigen in a pregnant woman
-Human Immunodeficiency Virus (HIV), including perinatal exposure
-Human Immunodeficiency Virus-related CD4+ counts and all viral loads
-Legionellosis [*Legionella pneumophila*]
-Leprosy, Hansen's disease [*Mycobacterium leprae*]
-Listeriosis [*Listeria monocytegenes*]
-Lyme disease [*Borrelia burgdorferi*]
-Malaria [*Plasmodium* species]
-Measles [Rubeola]*
-Mumps*
-*Neisseria meningitidis*, invasive disease, sterile site*
-Pertussis [*Bordetella pertussis*]*
-Plague [*Yersinia pestis*]*
-Pneumococcal disease, invasive [*Streptococcus pneumoniae*]
-Pneumocystis pneumonia [*Pneumocystis jiroveci* formerly *carinii*]
-Poliomyelitis [Polio]*
-Psittacosis [*Chlamydophilia psittaci*]*
-Rabies in humans or animals*
-Rocky Mountain Spotted Fever [*Rickettsia rickettsii*]
-Rubella, including Congenital Rubella Syndrome*
-Salmonellosis [*Salmonella* species] (report *S.* Typhi* within 24 hours)
-Shigellosis [*Shigella* species]
-Streptococcus Group A/B, invasive disease [*S. pyogenes/agalactiae*]
-Syphilis, including Congenital Syphilis Syndrome [*Treponema pallidum*]
-Tetanus [*Clostridium tetani*]
-Toxic-Shock Syndrome (TSS) [streptococcal or staphylococcal]
-Trichinosis [*Trichinella spiralis*]
-Tuberculosis disease [*Mycobacterium tuberculosis*]*
-Tuberculosis infection, latent
-Tularemia [*Francisella tularensis*]*
-Typhoid fever [*Salmonella* Typhi]*
-Typhus [*Rickettsia prowazekii*]*
-Varicella*
-Vibriosis [any *Vibrio* species]*
-Vancomycin Resistant Enterococci (VRE)
-Vancomycin Resistant *Staphylococcus aureus* (VRSA)*
-Yersiniosis [*Yersinia enterocolitica*]
-Any suspect outbreak, cluster of illness, or unusual occurrence of disease that may pose a threat to the public's health must be reported within 24 hours of recognition (please call reports in by phone)*

RECEIVED
MAY 16 2012
Infectious Disease Control

SCANNED
Initials: KB
Date: 7/25/12

EXHIBIT 2

EXETER HOSPITAL
5 Alumni Drive Exeter, NH 03833 603.778.7311
www.exeterhospital.com

Notice of Health Information Practices

Effective April 14, 2003

This notice describes how medical information about you may be used and disclosed and how you can get access to this information.

Please review it carefully.

I. Our policy regarding patient privacy

At Exeter Hospital, patient privacy is a priority. We follow Federal and State laws to maintain the confidentiality of your personal health information. This Notice describes how personal information about you and your health may be used and disclosed and how you can get access to this information. It also describes your rights and certain obligations we have regarding the use and disclosure of information about you and your health. We are required by law to give you this Notice and ask that you review it carefully. If you have any questions, please contact us at the telephone number or address listed at the end of the Notice.

II. Who will follow the practices described in this notice

The practices described in this Notice apply to all services provided by Exeter Hospital (including any satellite locations) and by the following:

- All physicians on the Medical Staff and all healthcare professionals on the Medical Associate Staff of Exeter Hospital with respect to the care they provide to you here at Exeter Hospital and the health information in your records here at the Hospital;
- Any healthcare professional authorized to enter information into your records here at the Hospital;
- All departments and units run by the Hospital;
- Any volunteer we allow to help you while you are receiving services at the Hospital; and
- All employees, staff and other Hospital personnel

These entities and caregivers may share health information about you with each other, as necessary, to carry out treatment, payment or healthcare operations in providing care to you in this integrated setting.

III. How we may use and reveal medical information about you

Each time a patient receives care at Exeter Hospital, a record of his or her visit is made. Typically, this record contains personal information (such as name, address, date of birth, social security number and insurance coverage), symptoms, examination and test results, diagnoses, treatment, and a plan for future care or treatment. It also may include sensitive information about you (such as HIV testing, or alcohol and drug abuse treatment). This information is referred to as personal health information and is maintained in your medical record. This record is an essential part of the healthcare we provide for you.

The following categories describe different ways that we use and disclose personal health information. For each category of uses or disclosures we explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed, but all of the ways in which we are permitted to use or disclose your personal health information will fall within one of these categories:

Treatment: We may use personal health information to provide you with medical treatment and to determine the course of treatment that should work best for you while you are at the Hospital. We may disclose your personal health information to doctors, nurses, technicians, medical students and other Hospital personnel who are on your healthcare team. For example, a doctor treating you for a broken arm may need to know if you have diabetes because it can slow the healing process. If you consent, we also may provide copies of your personal health information to your primary care physician, or another healthcare provider or specialist from whom you are receiving continued care which will assist them in providing that care.

Payment: If you consent, information about the services, treatment, medication, and supplies you received may be provided to your insurance company or other third party payer in order that we may receive payment. For example, we may need to give your health insurer information about a medical procedure we performed so that we may obtain payment for that procedure. If you consent, we may also inform your health plan about a treatment you are going to receive either to obtain prior approval for the treatment or to determine whether the treatment is covered by your insurance.

Healthcare Operations: We may use and disclose your personal health information for regular healthcare operations and business activities. These uses and disclosures are necessary to run the Hospital and make sure that patients receive quality care. For example, internal Hospital staff, members of the Medical Staff, medical students, managers, or members of the Quality Improvement Department may use information in your medical record to assess your care and outcomes, to monitor and evaluate the services we provide and see where we can make improvements, to determine whether new services should be offered, and for learning purposes.

Other Types of Uses for and Disclosures of Your Personal Health Information:

- ***Treatment Alternatives:*** We may use and disclose health information to tell you about or recommend possible treatment options or alternatives or other health related services which may be of interest to you.
- ***Appointment Reminders:*** We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment or medical care at the Hospital.
- *Health-Related Benefits and Services:* We may use and disclose health information to tell you about health-related benefits and services that may be of interest to you.
- ***Health-Related Benefits and Services:*** We may use and disclose health information to tell you about health-related benefits and services that may be of interest to you.
- ***Marketing:*** Exeter Hospital may use and disclose limited amounts of your personal health information in connection with marketing for the purpose of: furthering, managing or offering: treatment, alternative treatments, therapies, healthcare providers or locations of care. We may also use limited information to inform you of entities participating in a provider network or health plan, including the services offered by those providers; or the benefits covered by a health plan, including replacements to and enhancements for coverage under the plan.
- ***Fundraising:*** Exeter Hospital may use limited demographic information such as: your name, address, age and gender to contact you to support the Hospital's Development Program, which solicits donations, to expand and improve the services and programs Exeter Hospital provides to the community. If you do not wish to receive fundraising requests in support of Exeter Hospital, please send a letter to Exeter Hospital, Community Relations, 5 Alumni Drive, Exeter, NH 03833. In the event that you contact us with this request, all reasonable efforts shall be taken to ensure that you do not receive any future fundraising communication.

- ***Contract Services:*** We may share health information with third party business associates with whom we contract to perform various activities for our operations, such as a photocopy service responsible for copying medical records, or a coding or transcription service responsible for transmitting data for our health records. Whenever we have an arrangement between our organization and a business associate, we will limit the amount of health information that we provide to that which is necessary to accomplish the particular task.

Uses and Disclosures That We May Make Unless You Object: In the following situations, we may disclose your health information if you do not object to our doing so. If you do object, you must indicate in writing that you do not wish to have your personal health information used in this manner.

- ***Directory:*** We may include certain limited information about you in the inpatient directory while you are a patient at the Hospital to assist family, friends and visitors in finding you and learning about your general condition. This information includes your name, location in the Hospital, your general condition (e.g., stable, fair, etc.) and your religious affiliation. The directory information, except for your religious affiliation, may be released to people who ask for you by name.
- ***Clergy:*** Your religious affiliation may be given to a member of the clergy, such as a priest, minister or rabbi, even if he or she doesn't ask for you by name. This is so the clergy can visit you in the Hospital.
- ***Individuals Involved in Your Care:*** We may use or disclose certain relevant personal health information about you to family, friends or other persons you designate who are involved in your care or payment related to your health care. We may also use or disclose your information to notify or assist in notifying a family member, personal representative or another person responsible for your care of your location and general condition. We also may disclose personal health information about you to an authorized entity assisting in a disaster relief effort so that your family can be notified of your location and general condition.

Required Disclosures: We will disclose personal health information when required by federal, state and local law. For example, we must make disclosures when required by the Secretary of the Department of Health and Human Services to determine our compliance with the requirements of the federal Privacy Rule.

Other State and Federal Law Limitations: In situations where the laws in New Hampshire or other federal laws are more stringent or give patients more rights than federal privacy laws, such laws preempt the federal privacy law and we will abide by the other applicable state or federal law. For example, HIV testing information is subject to greater protections and more limited disclosure under New Hampshire law and information about alcohol and drug abuse treatment is subject to more limited disclosure requirements under another federal law.

Disclosures Not Requiring Your Authorization: There are limited times when we may use or disclose medical information without your authorization, such as in the situations listed below.

- ***Public Health:*** To public health or legal authorities responsible for preventing or controlling disease, injury or disability, or to report reactions to medications or problems with medical products;
- ***Abuse and Neglect Reporting:*** To government authorities, including protective service agencies, authorized to receive reports of abuse or neglect;
- ***Healthcare Oversight:*** To government oversight agencies for activities as authorized by law, including, for example, audits, investigations, inspections and licensure;
- ***Legal Proceedings:*** When required by a court order in a judicial or administrative proceeding;

- ***Law Enforcement:*** To law enforcement officials for certain enforcement purposes, including, for example, the reporting of certain types of wounds or injuries; or pursuant to a warrant, subpoena, or other legal process; or for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person;
- ***Coroners, Medical Examiners and Funeral Directors:*** To coroners, medical examiners, or funeral directors for purposes of identifying a deceased person, or determining a cause of death or to enable these parties to carry out their duties as required by law;
- ***Organ Donations and Transplants:*** To organ procurement organizations for purposes of organ or tissue donation and transplantation;
- ***Research:*** Under certain circumstances, for research approved by Exeter Hospital's Institutional Review Board (IRB) after it has reviewed the research proposal and established protocols to ensure the privacy of your health information;
- ***Public Safety/Duty to Warn:*** To warn of a serious threat to a clearly identified or reasonably identifiable person, or a serious threat of substantial damage to real property but only to threatened person or law enforcement to be able to help prevent the threat;
- ***Military and Veterans:*** If you are a member of the armed forces, as required by military command authorities, and to foreign military authorities, if you are foreign military personnel;
- ***National Security:*** To authorized federal officials for specialized government functions such as national security and intelligence; and
- ***Workers Compensation:*** As authorized by law in connection with Worker's Compensation programs.

Uses and Disclosures Specifically Authorized by You: All other uses and disclosures of your personal health information will be made only after we receive written authorization from you. You have the right to revoke any such authorization at any time in writing, except to the extent that we already have relied on it in making an authorized use or disclosure.

IV. Your health information rights

Although your medical record is maintained in the custody of the healthcare practitioner or facility that compiled it, the information belongs to you. With respect to the personal health information that we maintain about you, you have the right to:

- Obtain a paper copy of the Notice of Health Information Practices upon request, even if you have agreed to receive a copy in electronic form;
- Request additional restrictions on certain uses and disclosures of your health information, such as requesting that we not disclose the nature of a particular surgery you had, although we may or may not be required to agree to a restriction that you request;
- Request and receive confidential communications of your health information by alternative means or at alternative locations, such as contacting you only at work or only at home;
- Inspect and obtain a copy of your medical record, although, under certain circumstances, we are not required to agree to a request to inspect;
- Request that your medical record be amended if you feel it is incorrect or incomplete, although we are not required to agree with all requests;
- Obtain an accounting of certain disclosures of your health information made after April 14, 2003 for certain purposes other than treatment, payment, or healthcare operations; and
- Revoke your authorization to use or disclose personal health information except to the extent that action has already been taken.

If you wish to exercise any of these rights, please direct your request in writing to the Exeter Hospital Medical Record Department, 5 Alumni Drive, Exeter NH, Attention: Privacy Officer.

V. Our responsibilities

We have the following legal obligations regarding your personal health information:

- ***Privacy:*** We must maintain the privacy of your personal health information.
- ***Notice of Health Information Practices:*** We must provide you with this Notice as to our legal duties and privacy practices with respect to health information we collect and maintain about you.
- ***Follow Terms of Notice:*** All of the persons and entities listed in Section II above must follow the terms of this Notice.
- ***Changes to This Notice:*** We reserve the right to change our privacy practices and the terms of this Notice; these changes will apply to all personal health information which we already have about you as well as any information we receive or create in the future. Revised Notices will be available to patients at the Hospital, posted in the Hospital, and available on the Hospital's web page.
- ***Notification:*** We must notify you if we are unable to agree to a requested restriction.
- ***Communication Methods:*** We must accommodate reasonable requests that you may make to communicate personal health information by alternative means or at alternative locations.

To contact us

If you would like to exercise any of your rights listed in Section IV of this Notice or if you have questions and would like additional information, you may contact our Privacy Officer at:

Phone: 603.778.7311

Address: Exeter Hospital
Attn: Medical Record Department
5 Alumni Drive
Exeter, NH 03833

If you feel that any of your privacy rights have been violated, you may file a complaint with our Privacy Office at the above address or with the Secretary of the United States Department of Health and Human Services. **Any complaint should be submitted in writing. You will not be penalized and we will not retaliate against you in any way for filing a complaint.**

EXHIBIT 3

EXETER HOSPITAL

an exeter health resource | The Art of Wellness

August 21, 2012

Elizabeth Maynard, Esq.
Bureau of Legal Services
Department of Health and Human Services
State of New Hampshire
129 Pleasant Street
Concord, New Hampshire 03301-3857

Re: Access to Electronic Records

Dear Elizabeth:

This is in response to your letter of August 15, in addition to Sharon Alroy-Preis' e-mail of today asking about what claims of privilege we are making.

Patient Records

First, thank you for forwarding Exeter Hospital's End User Agreements, signed by members of the Department. To respond to your question, this agreement is the same that has been developed for vendors, non-employees and non-members of the medical staff, as the employees and medical staff members have other agreements that they are required to sign. Importantly, the latter are subject to a broad set of policies and procedures that address their responsibilities and provide sanctions for violations.

As you know, Exeter Hospital is a 'covered entity' under federal HIPAA statutes and regulations, and is subject to numerous requirements both under HIPAA and state laws for the protection of personal information within our possession. There are strong sanctions for failing to comply with these requirements. Our responsibilities include protecting this information from improper disclosure even to state and other governmental agencies. Even when disclosures are authorized, HIPAA requires limiting disclosures to the minimum necessary for use for an otherwise permissible purpose, in addition to our obligation to protect the security of records that are being viewed electronically. The latter requirements include protocols to assure that only the appropriate records are being accessed by persons for whom access is appropriate. We must also be able to provide an accounting of disclosures for patients who request such an accounting.

New Hampshire law relative to the protection of patient confidentiality is similar to HIPAA requirements:

> "I. Any protected health information provided to or acquired by the department under this chapter shall be released only with the informed consent of the individual or to those authorized persons having a legitimate need to acquire or use the information and then only so much of the information as is necessary for such persons to provide care and treatment to the individual who is the subject of the protected health

> information, investigate the cause of disease transmission in a particular case, or control the spread of the disease among the public. Any release of information under this section without the informed written consent of the individual shall be conditioned upon the protected health information remaining confidential.

We recognize that the state has certain examination rights of patient records with regard to communicable diseases; however, these are less than clear as to the breadth of information that may reasonably be released within the context of any individual investigation. Even the statute that you have explicitly cited requires that such investigations be conducted under rules adopted with due regard for the rights of persons and property. See RSA 141-C:9. We do not believe that the Department's general request for unbridled access to any and all records within the safekeeping of Exeter Hospital without advance disclosure to the hospital is consistent with your obligations for due regard to the rights of persons and property. Certainly, we do not believe that providing the state with such unfettered access is consistent with our confidentiality obligations to patients.

Our requests are reasonable, minimal and measured to ensure that the investigation is conducted with appropriate protections for the rights of persons and property. For example, providers are subject to an auditing requirement and the responsibility to notify patients who inquire as to who has had access to their records and for what purposes. Your disclosing to us in advance what records of Exeter Hospital's the Department wishes to review can't possibly be a violation of those patients' privacy rights, since the Hospital is the legal safekeeper of those privacy rights with respect to the Hospital's own records. On the other hand, if the Department requests a list of patients from us that meet certain parameters relevant to the investigation (such as, for example, records of deceased patients who had procedures in the CCL during the time period at issue in this investigation), that would satisfy our requirement as to the identification of the list of patients the records of which the Department seeks to access. This is the process that we have followed in providing you paper copies of records under circumstances in which the number requested is substantially less. Like you, we are anxious to understand the epidemiological reasons for the hepatitis-C outbreak in our patient community. We are unwilling, however, to violate the privacy and record security rights of all patients in aid of such an investigation. Due process, privacy rights and the security of confidential patient records of our patients must guide the ways in which this investigation proceeds. Both Exeter and the State of New Hampshire have this obligation. We urge you to reconsider your position expressed in your August 15 letter so that we can further your access to the requested information.

Quality Assurance Privilege

Hospital's have a statutory privilege under N.H. RSA 151:13-a for materials that relate to quality assurance investigations. In our review of relevant law, we have found nothing that would abrogate that privilege to allow the Department to procure both incident reports and investigatory materials that were generated by Exeter Hospital pursuant to its QA program, or work product related to it.

New Hampshire law specifically addresses the information that must be disclosed by a provider to DHHS during an investigation of incidents of communicable diseases, including certain privileged information. In relevant part, it provides as follows:

> I. Any protected health information provided to or acquired by the department under this chapter shall be released only with the informed consent of the individual or to those authorized persons having a legitimate need to acquire or use the information and then only so much of the information as is necessary for such persons to provide care and treatment to the individual who is the subject of the protected health information, investigate the cause of disease transmission in a particular case, or control the spread of the disease among the public. Any release of information under this section without the informed written consent of the individual shall be conditioned upon the protected health information remaining confidential.
>
> II. Analyses and compilations of data which do not disclose protected health information shall be available to the public under RSA 91-A.
>
> III. The physician-patient privilege shall not apply to information required to be reported or provided to the commissioner under this chapter.
>
> IV. The department shall acquire and retain only the minimum amount of information, specimens, and samples relating to individuals necessary to carry out its obligations under this chapter. The department shall adopt rules, pursuant to RSA 541-A, relative to the types of information, specimens, and samples to be acquired and the length of time such information, specimens, and samples shall be retained before being destroyed. Any genetic testing of specimens shall be limited to the viruses, bacteria, fungi, or other micro-organisms therein.

N.H. RSA 141-C:10 (I-IV).

Subsections I and IV above define what we are able to release and the limitations to which we're subject, Subsection II specifically provides that anything we provide to the Department that is not protected health is public information. Accordingly, we must take great care in terms of what information we release to the Department. This is why I had initially discussed with you the concept of allying the Department's epidemiological investigation with our QA process to assure that all information we have is protected. We would be willing to discuss this again in order to further the epidemiological process.

We hope to reach resolution on these important issues so that the Department's work may proceed with appropriate protections for all patients.

Sincerely yours,

Constance D. Sprauer, JD, MPH
Sr. Vice President for Legal Affairs
& General Counsel

cc: Kevin J. Callahan, CEO, Exeter Hospital
W. Scott O'Connell, Esq., Nixon Peabody
Nicholas Toumpas, Commissioner, DHHS
Dr. Jose Montero, Director of Public Health
Sharon Alroy-Preis, NH Epidemiologist
Frank Nachman, Esq., Chief Legal Counsel
Jeanne Herrick, NH Department of Justice

STATE OF NEW HAMPSHIRE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF OPERATIONS SUPPORT
BUREAU OF LEGAL SERVICES

Nicholas A. Toumpas
Commissioner

Mary P. Castelli
Senior Division Director

129 PLEASANT STREET, CONCORD, NH 03301-3857
603-271-9226 1-800-852-3345 Ext. 9226
FAX: 603-271-5590 TDD Access: 1-800-735-2964 www.dhhs.nh.gov

Transmitted Via Electronic Mail Only: csprauer@ehr.org

August 15, 2012

Constance Sprauer, Esq.
Exeter Health Resources
5 Alumni Drive
Exeter, NH 03833

RE: Follow up to Exeter Hospital request to sign End User Security Agreement

Dear Connie,

I am writing in response to Exeter Hospital's request for DPHS to sign its End User Security Agreement. The DHHS Legal Department has reviewed the terms of this Agreement. Overall, we see no reason not to sign the Agreement as written, as long as all Exeter Hospital employees, medical staff, contractors, vendors etc. are all signing the same agreement. I am presuming that DPHS will have access to all documents necessary to conduct its ongoing investigation. If there are documents for which DPHS will not have access, please let us know immediately and please explain why DPHS will not have access.

We do not see any valid reasons to require DPHS to provide a list of records we are planning to review and will not agree to this request. As you know, NH RSA 141-C:9, allows the Department of Health and Human Services to investigate incidents of communicable disease. These investigations include reviewing additional information and reports, including medical records. There is no obligation to disclose information in advance, and in fact doing so may be considered a violation of our requirement not to release protected health information pursuant to RSA 141-C:10.

We trust Exeter Hospital will fully cooperate with the DPHS as it continues its efforts to identify all patients infected with Hepatitis C as a result of the outbreak. I have attached copies of signed agreements from our staff at the DPHS/Bureau of Infectious Disease Control. Please telephone me with any questions.

Very sincerely yours,

Elizabeth Maynard, Esq.
Counsel for DPHS

cc: Sharon Alroy-Preis, State Epidemiologist
Chris Adamski, Bureau of Infectious Disease Control
Frank Nachman, Esq., Chief Legal Counsel
Jeanne Herrick, Esq., NH Department of Justice

EXETER HEALTH RESOURCES
5 Alumni Drive Exeter, NH 03833 603.778.7311

End User Security Agreement – Outside Individual Access

Purpose

The purpose of this agreement is to define standards and procedures for end users who have legitimate need to access data and systems from a device connected to Exeter Health Resources' (EHR) network. The overriding goal of this agreement is to protect the confidentiality, integrity and availability of the data and systems that resides within EHR's technology infrastructure and to secure protected health information (PHI) and personally identifiable information (PII) data in storage, in transit, and in use.

Applicability

This agreement applies to all EHR employees, members of the Exeter Hospital medical staff, contractors, vendors, and other individuals who utilize either company-owned or personally-owned devices to access, store, back up, or relocate any information stored on the EHR network. Such access to this confidential data is a privilege, not a right. This agreement applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet and desktop computers
- Mobile/cellular phones, Smart Phones, PDAs
- Home or personal computers used to access corporate resources.
- Removable media such as CD / DVD / Portable Media Devices.

Agreement and Appropriate Use

It is the responsibility of anyone who uses a device to access EHR data and resources, to adhere to and comply with all EHR privacy/security policies and applicable laws. .

User Device Security Details

General:

- Any device that is being used to access or store EHR data must adhere to the authentication requirements of EHR's IT department. In addition.
- All computers accessing information systems at Exeter Health Resources MUST have a working and up to date Anti-Virus solution. Contact the Help Desk (X6733) if you notice this is missing.
- Use of auto forwarding email from EHR email to personal email accounts is prohibited.
- Access to personal email accounts is permitted only on the guest network.
- Guest network access is permitted for non EHR-supplied devices only or specially marked terminals.
- It is prohibited to send or receive over the Internet or store any PHI / PII data on mobile devices or portable media unless the transmission and data storage is encrypted. Sending PHI/PII through Personal email is NOT permitted
- All Internet access from EHR devices is filtered and monitored.
- User shall not interfere with security features including patches, anti-virus, or other security configurations or software.

Passwords:

- My PASSWORD has the same authority as my signature and I am accountable for all work done under my code.
- I will not share my password with anyone for any reason.
- I understand that it is my responsibility to change any temporarily assigned passwords immediately.
- Information Services may issue a new password in the event of troubleshooting or logon issues and will set password to change at next logon, I will change my password immediately when the system prompts me to.
- I will NOT intentionally attempt to access any information not authorized for my use via my PASSWORD.
- If I have reason to believe that the confidentiality of my PASSWORD has been broken, I will immediately change my PASSWORD.

Workstation:

- I will log out of the system or secure my system with a password protected screensaver before I leave the workstation.
- .

Removable Media:

- ALL portable media containing PHI / PII MUST be encrypted unless instructed otherwise by IS.
- All Portable media must be destroyed or properly deleted per the media reuse agreement.

Remote Access:

- Tethering, sharing, or otherwise combining networks on any device is prohibited.
- Remote cloud services such as "Mobile-Me" and Microsoft Live Sync are not permitted for backing up, storing, accessing or sharing data.
- Remote use of EHR applications or access to data is only permitted through secure encrypted sessions and must be an EHR sanctioned remote access solution.

Help & Support

EHR's IS department will support its approved hardware and software. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned installed hardware or software without the express approval of EHR's IS department. Requests can be sent to the Help Desk Mailbox or Helpdesk@ehr.org and the requestor will be contacted.

Agreement Non-Compliance

I have read and understand the above End User Security Agreement, and consent to adhere to the rules outlined therein. I will report any breach or non compliance of this agreement.

Karin Salome — Employee Printed Name

RN — Department / Title

Karin Salome — Employee Signature

8/10/12 — Date

EXETER HEALTH RESOURCES
5 Alumni Drive Exeter, NH 03833 603.778.7311

End User Security Agreement – Outside Individual Access

Purpose

The purpose of this agreement is to define standards and procedures for end users who have legitimate need to access data and systems from a device connected to Exeter Health Resources' (EHR) network. The overriding goal of this agreement is to protect the confidentiality, integrity and availability of the data and systems that resides within EHR's technology infrastructure and to secure protected health information (PHI) and personally identifiable information (PII) data in storage, in transit, and in use.

Applicability

This agreement applies to all EHR employees, members of the Exeter Hospital medical staff, contractors, vendors, and other individuals who utilize either company-owned or personally-owned devices to access, store, back up, or relocate any information stored on the EHR network. Such access to this confidential data is a privilege, not a right. This agreement applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet and desktop computers
- Mobile/cellular phones, Smart Phones, PDAs
- Home or personal computers used to access corporate resources.
- Removable media such as CD / DVD / Portable Media Devices.

Agreement and Appropriate Use

It is the responsibility of anyone who uses a device to access EHR data and resources, to adhere to and comply with all EHR privacy/security policies and applicable laws. .

User Device Security Details

General:

- Any device that is being used to access or store EHR data must adhere to the authentication requirements of EHR's IT department. In addition.
- All computers accessing information systems at Exeter Health Resources MUST have a working and up to date Anti-Virus solution. Contact the Help Desk (X6733) if you notice this is missing.
- Use of auto forwarding email from EHR email to personal email accounts is prohibited.
- Access to personal email accounts is permitted only on the guest network.
- Guest network access is permitted for non EHR-supplied devices only or specially marked terminals.
- It is prohibited to send or receive over the Internet or store any PHI / PII data on mobile devices or portable media unless the transmission and data storage is encrypted. Sending PHI/PII through Personal email is NOT permitted
- All Internet access from EHR devices is filtered and monitored.
- User shall not interfere with security features including patches, anti-virus, or other security configurations or software.

Passwords:

- My PASSWORD has the same authority as my signature and I am accountable for all work done under my code.
- I will not share my password with anyone for any reason.
- I understand that it is my responsibility to change any temporarily assigned passwords immediately.
- Information Services may issue a new password in the event of troubleshooting or logon issues and will set password to change at next logon, I will change my password immediately when the system prompts me to.
- I will NOT intentionally attempt to access any information not authorized for my use via my PASSWORD.
- If I have reason to believe that the confidentiality of my PASSWORD has been broken, I will immediately change my PASSWORD.

Workstation:

- I will log out of the system or secure my system with a password protected screensaver before I leave the workstation.
- .

Removable Media:

- ALL portable media containing PHI / PII MUST be encrypted unless instructed otherwise by IS.
- All Portable media must be destroyed or properly deleted per the media reuse agreement.

Remote Access:

- Tethering, sharing, or otherwise combining networks on any device is prohibited.
- Remote cloud services such as "Mobile-Me" and Microsoft Live Sync are not permitted for backing up, storing, accessing or sharing data.
- Remote use of EHR applications or access to data is only permitted through secure encrypted sessions and must be an EHR sanctioned remote access solution.

Help & Support

EHR's IS department will support its approved hardware and software. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned installed hardware or software without the express approval of EHR's IS department. Requests can be sent to the Help Desk Mailbox or Helpdesk@ehr.org and the requestor will be contacted.

Agreement Non-Compliance

I have read and understand the above End User Security Agreement, and consent to adhere to the rules outlined therein. I will report any breach or non compliance of this agreement.

Erin Metcalf
Employee Printed Name

NH DHHS, DPHS / HIV Surveillance Coordinator
Department / Title

Erin Metcalf
Employee Signature

8/9/12
Date

EXETER HEALTH RESOURCES
5 Alumni Drive Exeter, NH 03833 603.778.7311

End User Security Agreement – Outside Individual Access

Purpose

The purpose of this agreement is to define standards and procedures for end users who have legitimate need to access data and systems from a device connected to Exeter Health Resources' (EHR) network. The overriding goal of this agreement is to protect the confidentiality, integrity and availability of the data and systems that resides within EHR's technology infrastructure and to secure protected health information (PHI) and personally identifiable information (PII) data in storage, in transit, and in use.

Applicability

This agreement applies to all EHR employees, members of the Exeter Hospital medical staff, contractors, vendors, and other individuals who utilize either company-owned or personally-owned devices to access, store, back up, or relocate any information stored on the EHR network. Such access to this confidential data is a privilege, not a right. This agreement applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet and desktop computers
- Mobile/cellular phones, Smart Phones, PDAs
- Home or personal computers used to access corporate resources.
- Removable media such as CD / DVD / Portable Media Devices.

Agreement and Appropriate Use

It is the responsibility of anyone who uses a device to access EHR data and resources, to adhere to and comply with all EHR privacy/security policies and applicable laws. .

User Device Security Details

General:

- Any device that is being used to access or store EHR data must adhere to the authentication requirements of EHR's IT department. In addition.
- All computers accessing information systems at Exeter Health Resources MUST have a working and up to date Anti-Virus solution. Contact the Help Desk (X6733) if you notice this is missing.
- Use of auto forwarding email from EHR email to personal email accounts is prohibited.
- Access to personal email accounts is permitted only on the guest network.
- Guest network access is permitted for non EHR-supplied devices only or specially marked terminals.
- It is prohibited to send or receive over the Internet or store any PHI / PII data on mobile devices or portable media unless the transmission and data storage is encrypted. Sending PHI/PII through Personal email is NOT permitted
- All Internet access from EHR devices is filtered and monitored.
- User shall not interfere with security features including patches, anti-virus, or other security configurations or software.

Passwords:

- My PASSWORD has the same authority as my signature and I am accountable for all work done under my code.
- I will not share my password with anyone for any reason.
- I understand that it is my responsibility to change any temporarily assigned passwords immediately.
- Information Services may issue a new password in the event of troubleshooting or logon Issues and will set password to change at next logon, I will change my password immediately when the system prompts me to.
- I will NOT intentionally attempt to access any information not authorized for my use via my PASSWORD.
- If I have reason to believe that the confidentiality of my PASSWORD has been broken, I will immediately change my PASSWORD.

Workstation:

- I will log out of the system or secure my system with a password protected screensaver before I leave the workstation.

- .

Removable Media:

- ALL portable media containing PHI / PII MUST be encrypted unless instructed otherwise by IS.
- All Portable media must be destroyed or properly deleted per the media reuse agreement.

Remote Access:

- Tethering, sharing, or otherwise combinlng networks on any device is prohibited.
- Remote cloud services such as "Mobile-Me" and Microsoft Live Sync are not permitted for backing up, storing, accessing or sharing data.
- Remote use of EHR applications or access to data is only permitted through secure encrypted sessions and must be an EHR sanctioned remote access solution.

Help & Support

EHR's IS department will support its approved hardware and software. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned installed hardware or software without the express approval of EHR's IS department. Requests can be sent to the Help Desk Mailbox or Helpdesk@ehr.org and the requestor will be contacted.

Agreement Non-Compliance

I have read and understand the above End User Security Agreement, and consent to adhere to the rules outlined therein. I will report any breach or non compliance of this agreement.

Sarah Krycki
Employee Printed Name

Nurse Specialist
Department / Title

Sarah Krycki
Employee Signature

August 9 2012
Date

EXETER HEALTH RESOURCES
5 Alumni Drive Exeter, NH 03833 603.778.7311

End User Security Agreement – Outside Individual Access

Purpose

The purpose of this agreement is to define standards and procedures for end users who have legitimate need to access data and systems from a device connected to Exeter Health Resources' (EHR) network. The overriding goal of this agreement is to protect the confidentiality, integrity and availability of the data and systems that resides within EHR's technology infrastructure and to secure protected health information (PHI) and personally identifiable information (PII) data in storage, in transit, and in use.

Applicability

This agreement applies to all EHR employees, members of the Exeter Hospital medical staff, contractors, vendors, and other individuals who utilize either company-owned or personally-owned devices to access, store, back up, or relocate any information stored on the EHR network. Such access to this confidential data is a privilege, not a right. This agreement applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet and desktop computers
- Mobile/cellular phones, Smart Phones, PDAs
- Home or personal computers used to access corporate resources.
- Removable media such as CD / DVD / Portable Media Devices.

Agreement and Appropriate Use

It is the responsibility of anyone who uses a device to access EHR data and resources, to adhere to and comply with all EHR privacy/security policies and applicable laws. .

User Device Security Details

General:

- Any device that is being used to access or store EHR data must adhere to the authentication requirements of EHR's IT department. In addition.
- All computers accessing information systems at Exeter Health Resources MUST have a working and up to date Anti-Virus solution. Contact the Help Desk (X6733) if you notice this is missing.
- Use of auto forwarding email from EHR email to personal email accounts is prohibited.
- Access to personal email accounts is permitted only on the guest network.
- Guest network access is permitted for non EHR-supplied devices only or specially marked terminals.
- It is prohibited to send or receive over the Internet or store any PHI / PII data on mobile devices or portable media unless the transmission and data storage is encrypted. Sending PHI/PII through Personal email is NOT permitted
- All Internet access from EHR devices is filtered and monitored.
- User shall not interfere with security features including patches, anti-virus, or other security configurations or software.

Passwords:

- My PASSWORD has the same authority as my signature and I am accountable for all work done under my code.
- I will not share my password with anyone for any reason.
- I understand that it is my responsibility to change any temporarily assigned passwords immediately.
- Information Services may issue a new password in the event of troubleshooting or logon issues and will set password to change at next logon, I will change my password immediately when the system prompts me to.
- I will NOT intentionally attempt to access any information not authorized for my use via my PASSWORD.
- If I have reason to believe that the confidentiality of my PASSWORD has been broken, I will immediately change my PASSWORD.

Workstation:

- I will log out of the system or secure my system with a password protected screensaver before I leave the workstation.

- .

Removable Media:

- ALL portable media containing PHI / PII MUST be encrypted unless instructed otherwise by IS.
- All Portable media must be destroyed or properly deleted per the media reuse agreement.

Remote Access:

- Tethering, sharing, or otherwise combining networks on any device is prohibited.
- Remote cloud services such as "Mobile-Me" and Microsoft Live Sync are not permitted for backing up, storing, accessing or sharing data.
- Remote use of EHR applications or access to data is only permitted through secure encrypted sessions and must be an EHR sanctioned remote access solution.

Help & Support

EHR's IS department will support its approved hardware and software. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned installed hardware or software without the express approval of EHR's IS department. Requests can be sent to the Help Desk Mailbox or Helpdesk@ehr.org and the requestor will be contacted.

Agreement Non-Compliance

I have read and understand the above End User Security Agreement, and consent to adhere to the rules outlined therein. I will report any breach or non compliance of this agreement.

Steffany Cavallo
Employee Printed Name

Employee Signature

NHDHHS / Infectious Disease Epidemiologist
Department / Title

8/9/2012
Date

EXETER HEALTH RESOURCES
5 Alumni Drive Exeter, NH 03833 603.778.7311

End User Security Agreement – Outside Individual Access

Purpose

The purpose of this agreement is to define standards and procedures for end users who have legitimate need to access data and systems from a device connected to Exeter Health Resources' (EHR) network. The overriding goal of this agreement is to protect the confidentiality, integrity and availability of the data and systems that resides within EHR's technology infrastructure and to secure protected health information (PHI) and personally identifiable information (PII) data in storage, in transit, and in use.

Applicability

This agreement applies to all EHR employees, members of the Exeter Hospital medical staff, contractors, vendors, and other individuals who utillze either company-owned or personally-owned devices to access, store, back up, or relocate any information stored on the EHR network. Such access to this confidential data is a privilege, not a right. This agreement applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet and desktop computers
- Mobile/cellular phones, Smart Phones, PDAs
- Home or personal computers used to access corporate resources.
- Removable media such as CD / DVD / Portable Media Devices.

Agreement and Appropriate Use

It is the responsibility of anyone who uses a device to access EHR data and resources, to adhere to and comply with all EHR privacy/security policies and applicable laws. .

User Device Security Details

General:

- Any device that is being used to access or store EHR data must adhere to the authentication requirements of EHR's IT department. In addition.
- All computers accessing information systems at Exeter Health Resources MUST have a working and up to date Anti-Virus solution. Contact the Help Desk (X6733) if you notice this is missing.
- Use of auto forwarding email from EHR email to personal email accounts is prohibited.
- Access to personal email accounts is permitted only on the guest network.
- Guest network access is permitted for non EHR-supplied devices only or specially marked terminals.
- It is prohibited to send or receive over the Internet or store any PHI / PII data on mobile devices or portable media unless the transmission and data storage is encrypted. Sending PHI/PII through Personal email is NOT permitted
- All Internet access from EHR devices is filtered and monitored.
- User shall not interfere with security features including patches, anti-virus, or other security configurations or software.

Passwords:

- My PASSWORD has the same authority as my signature and I am accountable for all work done under my code.
- I will not share my password with anyone for any reason.
- I understand that it is my responsibility to change any temporarily assigned passwords immediately.
- Information Services may issue a new password in the event of troubleshooting or logon issues and will set password to change at next logon, I will change my password immediately when the system prompts me to.
- I will NOT intentionally attempt to access any information not authorized for my use via my PASSWORD.
- If I have reason to believe that the confidentiality of my PASSWORD has been broken, I will immediately change my PASSWORD.

Workstation:

- I will log out of the system or secure my system with a password protected screensaver before I leave the workstation.
- .

Removable Media:

- ALL portable media containing PHI / PII MUST be encrypted unless instructed otherwise by IS.
- All Portable media must be destroyed or properly deleted per the media reuse agreement.

Remote Access:

- Tethering, sharing, or otherwise combining networks on any device is prohibited.
- Remote cloud services such as "Mobile-Me" and Microsoft Live Sync are not permitted for backing up, storing, accessing or sharing data.
- Remote use of EHR applications or access to data is only permitted through secure encrypted sessions and must be an EHR sanctioned remote access solution.

Help & Support

EHR's IS department will support its approved hardware and software. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned installed hardware or software without the express approval of EHR's IS department. Requests can be sent to the Help Desk Mailbox or Helpdesk@ehr.org and the requestor will be contacted.

Agreement Non-Compliance

I have read and understand the above End User Security Agreement, and consent to adhere to the rules outlined therein. I will report any breach or non compliance of this agreement.

Katrina Hansen
Employee Printed Name

HAI program coordinator
Department / Title

Employee Signature

8/2/12
Date

EXETER HEALTH RESOURCES
5 Alumni Drive Exeter, NH 03833 603.778.7311

End User Security Agreement – Outside Individual Access

Purpose

The purpose of this agreement is to define standards and procedures for end users who have legitimate need to access data and systems from a device connected to Exeter Health Resources' (EHR) network. The overriding goal of this agreement is to protect the confidentiality, integrity and availability of the data and systems that resides within EHR's technology infrastructure and to secure protected health information (PHI) and personally identifiable information (PII) data in storage, in transit, and in use.

Applicability

This agreement applies to all EHR employees, members of the Exeter Hospital medical staff, contractors, vendors, and other individuals who utilize either company-owned or personally-owned devices to access, store, back up, or relocate any information stored on the EHR network. Such access to this confidential data is a privilege, not a right. This agreement applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet and desktop computers
- Mobile/cellular phones, Smart Phones, PDAs
- Home or personal computers used to access corporate resources.
- Removable media such as CD / DVD / Portable Media Devices.

Agreement and Appropriate Use

It is the responsibility of anyone who uses a device to access EHR data and resources, to adhere to and comply with all EHR privacy/security policies and applicable laws. .

User Device Security Details

General:

- Any device that is being used to access or store EHR data must adhere to the authentication requirements of EHR's IT department. In addition.
- All computers accessing information systems at Exeter Health Resources MUST have a working and up to date Anti-Virus solution. Contact the Help Desk (X6733) if you notice this is missing.
- Use of auto forwarding email from EHR email to personal email accounts is prohibited.
- Access to personal email accounts is permitted only on the guest network.
- Guest network access is permitted for non EHR-supplied devices only or specially marked terminals.
- It is prohibited to send or receive over the Internet or store any PHI / PII data on mobile devices or portable media unless the transmission and data storage is encrypted. Sending PHI/PII through Personal email is NOT permitted
- All Internet access from EHR devices is filtered and monitored.
- User shall not interfere with security features including patches, anti-virus, or other security configurations or software.

Passwords:

- My PASSWORD has the same authority as my signature and I am accountable for all work done under my code.
- I will not share my password with anyone for any reason.
- I understand that it is my responsibility to change any temporarily assigned passwords immediately.
- Information Services may issue a new password in the event of troubleshooting or logon issues and will set password to change at next logon, I will change my password immediately when the system prompts me to.
- I will NOT intentionally attempt to access any information not authorized for my use via my PASSWORD.
- If I have reason to believe that the confidentiality of my PASSWORD has been broken, I will immediately change my PASSWORD.

Workstation:

- I will log out of the system or secure my system with a password protected screensaver before I leave the workstation.

- .

Removable Media:

- ALL portable media containing PHI / PII MUST be encrypted unless instructed otherwise by IS.
- All Portable media must be destroyed or properly deleted per the media reuse agreement.

Remote Access:

- Tethering, sharing, or otherwise combining networks on any device is prohibited.
- Remote cloud services such as "Mobile-Me" and Microsoft Live Sync are not permitted for backing up, storing, accessing or sharing data.
- Remote use of EHR applications or access to data is only permitted through secure encrypted sessions and must be an EHR sanctioned remote access solution.

Help & Support

EHR's IS department will support its approved hardware and software. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned installed hardware or software without the express approval of EHR's IS department. Requests can be sent to the Help Desk Mailbox or Helpdesk@ehr.org and the requestor will be contacted.

Agreement Non-Compliance

I have read and understand the above End User Security Agreement, and consent to adhere to the rules outlined therein. I will report any breach or non compliance of this agreement.

Abigail Matheson
Employee Printed Name

Abigail Matheson
Employee Signature

NHDHHS Surveillance Epidemiology Program Manager
Department / Title

8/2/12
Date

EXETER HEALTH RESOURCES
5 Alumni Drive Exeter, NH 03833 603.778.7311

End User Security Agreement – Outside Individual Access

Purpose

The purpose of this agreement is to define standards and procedures for end users who have legitimate need to access data and systems from a device connected to Exeter Health Resources' (EHR) network. The overriding goal of this agreement is to protect the confidentiality, integrity and availability of the data and systems that resides within EHR's technology infrastructure and to secure protected health information (PHI) and personally identifiable information (PII) data in storage, in transit, and in use.

Applicability

This agreement applies to all EHR employees, members of the Exeter Hospital medical staff, contractors, vendors, and other individuals who utilize either company-owned or personally-owned devices to access, store, back up, or relocate any information stored on the EHR network. Such access to this confidential data is a privilege, not a right. This agreement applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet and desktop computers
- Mobile/cellular phones, Smart Phones, PDAs
- Home or personal computers used to access corporate resources.
- Removable media such as CD / DVD / Portable Media Devices.

Agreement and Appropriate Use

It is the responsibility of anyone who uses a device to access EHR data and resources, to adhere to and comply with all EHR privacy/security policies and applicable laws. .

User Device Security Details

General:

- Any device that is being used to access or store EHR data must adhere to the authentication requirements of EHR's IT department. In addition.
- All computers accessing information systems at Exeter Health Resources MUST have a working and up to date Anti-Virus solution. Contact the Help Desk (X6733) if you notice this is missing.
- Use of auto forwarding email from EHR email to personal email accounts is prohibited.
- Access to personal email accounts is permitted only on the guest network.
- Guest network access is permitted for non EHR-supplied devices only or specially marked terminals.
- It is prohibited to send or receive over the Internet or store any PHI / PII data on mobile devices or portable media unless the transmission and data storage is encrypted. Sending PHI/PII through Personal email is NOT permitted
- All Internet access from EHR devices is filtered and monitored.
- User shall not interfere with security features including patches, anti-virus, or other security configurations or software.

Passwords:

- My PASSWORD has the same authority as my signature and I am accountable for all work done under my code.
- I will not share my password with anyone for any reason.
- I understand that it is my responsibility to change any temporarily assigned passwords immediately.
- Information Services may issue a new password in the event of troubleshooting or logon issues and will set password to change at next logon, I will change my password immediately when the system prompts me to.
- I will NOT intentionally attempt to access any information not authorized for my use via my PASSWORD.
- If I have reason to believe that the confidentiality of my PASSWORD has been broken, I will immediately change my PASSWORD.

Workstation:

- I will log out of the system or secure my system with a password protected screensaver before I leave the workstation.
- .

Removable Media:

- ALL portable media containing PHI / PII MUST be encrypted unless instructed otherwise by IS.
- All Portable media must be destroyed or properly deleted per the media reuse agreement.

Remote Access:

- Tethering, sharing, or otherwise combining networks on any device is prohibited.
- Remote cloud services such as "Mobile-Me" and Microsoft Live Sync are not permitted for backing up, storing, accessing or sharing data.
- Remote use of EHR applications or access to data is only permitted through secure encrypted sessions and must be an EHR sanctioned remote access solution.

Help & Support

EHR's IS department will support its approved hardware and software. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned installed hardware or software without the express approval of EHR's IS department. Requests can be sent to the Help Desk Mailbox or Helpdesk@ehr.org and the requestor will be contacted.

Agreement Non-Compliance

I have read and understand the above End User Security Agreement, and consent to adhere to the rules outlined therein. I will report any breach or non compliance of this agreement.

Elizabeth R. Daly
Employee Printed Name

NH DHHS
Department / Title

Employee Signature

08/02/12
Date

EXETER HEALTH RESOURCES
5 Alumni Drive Exeter, NH 03833 603.778.7311

End User Security Agreement – Outside Individual Access

Purpose

The purpose of this agreement is to define standards and procedures for end users who have legitimate need to access data and systems from a device connected to Exeter Health Resources' (EHR) network. The overriding goal of this agreement is to protect the confidentiality, integrity and availability of the data and systems that resides within EHR's technology infrastructure and to secure protected health information (PHI) and personally identifiable information (PII) data in storage, in transit, and in use.

Applicability

This agreement applies to all EHR employees, members of the Exeter Hospital medical staff, contractors, vendors, and other individuals who utilize either company-owned or personally-owned devices to access, store, back up, or relocate any information stored on the EHR network. Such access to this confidential data is a privilege, not a right. This agreement applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet and desktop computers
- Mobile/cellular phones, Smart Phones, PDAs
- Home or personal computers used to access corporate resources.
- Removable media such as CD / DVD / Portable Media Devices.

Agreement and Appropriate Use

It is the responsibility of anyone who uses a device to access EHR data and resources, to adhere to and comply with all EHR privacy/security policies and applicable laws. .

User Device Security Details

General:

- Any device that is being used to access or store EHR data must adhere to the authentication requirements of EHR's IT department. In addition.
- All computers accessing information systems at Exeter Health Resources MUST have a working and up to date Anti-Virus solution. Contact the Help Desk (X6733) if you notice this is missing.
- Use of auto forwarding email from EHR email to personal email accounts is prohibited.
- Access to personal email accounts is permitted only on the guest network.
- Guest network access is permitted for non EHR-supplied devices only or specially marked terminals.
- It is prohibited to send or receive over the Internet or store any PHI / PII data on mobile devices or portable media unless the transmission and data storage is encrypted. Sending PHI/PII through Personal email is NOT permitted
- All Internet access from EHR devices is filtered and monitored.
- User shall not interfere with security features including patches, anti-virus, or other security configurations or software.

Passwords:

- My PASSWORD has the same authority as my signature and I am accountable for all work done under my code.
- I will not share my password with anyone for any reason.
- I understand that it is my responsibility to change any temporarily assigned passwords immediately.
- Information Services may issue a new password in the event of troubleshooting or logon issues and will set password to change at next logon, I will change my password immediately when the system prompts me to.
- I will NOT intentionally attempt to access any information not authorized for my use via my PASSWORD.
- If I have reason to believe that the confidentiality of my PASSWORD has been broken, I will immediately change my PASSWORD.

Workstation:

- I will log out of the system or secure my system with a password protected screensaver before I leave the workstation.
- .

Removable Media:

- ALL portable media containing PHI / PII MUST be encrypted unless instructed otherwise by IS.
- All Portable media must be destroyed or properly deleted per the media reuse agreement.

Remote Access:

- Tethering, sharing, or otherwise combining networks on any device is prohibited.
- Remote cloud services such as "Mobile-Me" and Microsoft Live Sync are not permitted for backing up, storing, accessing or sharing data.
- Remote use of EHR applications or access to data is only permitted through secure encrypted sessions and must be an EHR sanctioned remote access solution.

Help & Support

EHR's IS department will support its approved hardware and software. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned installed hardware or software without the express approval of EHR's IS department. Requests can be sent to the Help Desk Mailbox or Helpdesk@ehr.org and the requestor will be contacted.

Agreement Non-Compliance

I have read and understand the above End User Security Agreement, and consent to adhere to the rules outlined therein. I will report any breach or non compliance of this agreement.

Kim Budde
Employee Printed Name

DHHS / Infectious Disease Epidemiologist
Department / Title

Kim Budde
Employee Signature

8/2/12
Date

EXHIBIT 4

DISCLOSURES FOR PUBLIC HEALTH ACTIVITIES
[45 CFR 164.512(b)]

Background

The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information to carry out their public health mission. The Rule also recognizes that public health reports made by covered entities are an important means of identifying threats to the health and safety of the public at large, as well as individuals. Accordingly, the Rule permits covered entities to disclose protected health information without authorization for specified public health purposes.

How the Rule Works

General Public Health Activities. The Privacy Rule permits covered entities to disclose protected health information, without authorization, to public health authorities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions. See 45 CFR 164.512(b)(1)(i). Also, covered entities may, at the direction of a public health authority, disclose protected health information to a foreign government agency that is acting in collaboration with a public health authority. See 45 CFR 164.512(b)(1)(i). Covered entities who are also a public health authority may use, as well as disclose, protected health information for these public health purposes. See 45 CFR 164.512(b)(2).

A "public health authority" is an agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. See 45 CFR 164.501. Examples of a public health authority include State and local health departments, the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention, and the Occupational Safety and Health Administration (OSHA).

Generally, covered entities are required reasonably to limit the protected health information disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose. However, covered entities are not required to make a minimum necessary determination for public health disclosures that are made pursuant to an individual's authorization, or for disclosures that are required by other law. See 45 CFR 164.502(b). For disclosures to a public health authority, covered entities may reasonably rely on

a minimum necessary determination made by the public health authority in requesting the protected health information. See 45 CFR 164.514(d)(3)(iii)(A). For routine and recurring public health disclosures, covered entities may develop standard protocols, as part of their minimum necessary policies and procedures, that address the types and amount of protected health information that may be disclosed for such purposes. See 45 CFR 164.514(d)(3)(i).

Other Public Health Activities. The Privacy Rule recognizes the important role that persons or entities other than public health authorities play in certain essential public health activities. Accordingly, the Rule permits covered entities to disclose protected health information, without authorization, to such persons or entities for the public health activities discussed below.

- Child abuse or neglect. Covered entities may disclose protected health information to report known or suspected child abuse or neglect, if the report is made to a public health authority or other appropriate government authority that is authorized by law to receive such reports. For instance, the social services department of a local government might have legal authority to receive reports of child abuse or neglect, in which case, the Privacy Rule would permit a covered entity to report such cases to that authority without obtaining individual authorization. Likewise, a covered entity could report such cases to the police department when the police department is authorized by law to receive such reports. See 45 CFR 164.512(b)(1)(ii). See also 45 CFR 512(c) for information regarding disclosures about adult victims of abuse, neglect, or domestic violence.

- Quality, safety or effectiveness of a product or activity regulated by the FDA. Covered entities may disclose protected health information to a person subject to FDA jurisdiction, for public health purposes related to the quality, safety or effectiveness of an FDA-regulated product or activity for which that person has responsibility. Examples of purposes or activities for which such disclosures may be made include, but are not limited to:

  - Collecting or reporting adverse events (including similar reports regarding food and dietary supplements), product defects or problems (including problems regarding use or labeling), or biological product deviations;
  - Tracking FDA-regulated products;
  - Enabling product recalls, repairs, replacement or lookback (which includes locating and notifying individuals who received recalled or withdrawn products or products that are the subject of lookback); and
  - Conducting post-marketing surveillance.

See 45 CFR 164.512(b)(1)(iii). The "person" subject to the jurisdiction of the FDA does not have to be a specific individual. Rather, it can be an individual or an entity, such as a partnership, corporation, or association. Covered entities may identify the party or parties responsible for an FDA-regulated product from the product label, from written material that accompanies the product (know as labeling), or from sources of labeling, such as the Physician's Desk Reference.

- Persons at risk of contracting or spreading a disease. A covered entity may disclose protected health information to a person who is at risk of contracting or spreading a disease or condition if other law authorizes the covered entity to notify such individuals as necessary to carry out public health interventions or investigations. For example, a covered health care provider may disclose protected health information as needed to notify a person that (s)he has been exposed to a communicable disease if the covered entity is legally authorized to do so to prevent or control the spread of the disease. See 45 CFR 164.512(b)(1)(iv).

- Workplace medical surveillance. A covered health care provider who provides a health care service to an individual at the request of the individual's employer, or provides the service in the capacity of a member of the employer's workforce, may disclose the individual's protected health information to the employer for the purposes of workplace medical surveillance or the evaluation of work-related illness and injuries to the extent the employer needs that information to comply with OSHA, the Mine Safety and Health Administration (MSHA), or the requirements of State laws having a similar purpose. The information disclosed must be limited to the provider's findings regarding such medical surveillance or work-related illness or injury. The covered health care provider must provide the individual with written notice that the information will be disclosed to his or her employer (or the notice may be posted at the worksite if that is where the service is provided). See 45 CFR 164.512(b)(1)(v).

Frequently Asked Questions

To see Privacy Rule FAQs, click the desired link below:

FAQs on Public Health Uses and Disclosures

FAQs on ALL Privacy Rule Topics

(You can also go to http://answers.hhs.gov/cgi-bin/hhs.cfg/php/enduser/std_alp.php, then select "Privacy of Health Information/HIPAA" from the Category drop down list and click the Search button.)

EXHIBIT 5

CDC Home | Search | Health Topics A-Z

MMWR

Early Release
April 11, 2003 / 52;1-12

HIPAA Privacy Rule and Public Health

Guidance from CDC and the U.S. Department of Health and Human Services*

The material in this report originated in the Epidemiology Program Office, Stephen B. Thacker, M.D., M.Sc., Director.

Summary

New national health information privacy standards have been issued by the U.S. Department of Health and Human Services (DHHS), pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The new regulations provide protection for the privacy of certain individually identifiable health data, referred to as protected health information (PHI). Balancing the protection of individual health information with the need to protect public health, the Privacy Rule expressly permits disclosures without individual authorization to public health authorities authorized by law to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to public health surveillance, investigation, and intervention.

Public health practice often requires the acquisition, use, and exchange of PHI to perform public health activities (e.g., public health surveillance, program evaluation, terrorism preparedness, outbreak investigations, direct health services, and public health research). Such information enables public health authorities to implement mandated activities (e.g., identifying, monitoring, and responding to death, disease, and disability among populations) and accomplish public health objectives. Public health authorities have a long history of respecting the confidentiality of PHI, and the majority of states as well as the federal government have laws that govern the use of, and serve to protect, identifiable information collected by public health authorities.

The purpose of this report is to help public health agencies and others understand and interpret their responsibilities under the Privacy Rule. Elsewhere, comprehensive DHHS guidance is located at the HIPAA website of the Office for Civil Rights (http://www.hhs.gov/ocr/hipaa/).

Introduction

The shift of medical records from paper to electronic formats has increased the potential for individuals to access, use, and disclose sensitive personal health data. Although protecting individual privacy is a long-standing tradition among health-care providers and public health practitioners in the United States, previous legal protections at the federal, tribal, state, and local levels were inconsistent and inadequate. A patchwork of laws provided narrow privacy protections for selected health data and certain keepers of that data (*1*).

The U.S. Department of Health and Human Services (DHHS) has addressed these concerns with new privacy standards that set a national minimum of basic protections, while balancing individual needs with

those of society. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was adopted to ensure health insurance coverage after leaving an employer and also to provide standards for facilitating health-care--related electronic transactions. To improve the efficiency and effectiveness of the health-care system, HIPAA included administrative simplification provisions that required DHHS to adopt national standards for electronic health-care transactions (*2*). At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated adoption of federal privacy protections for certain individually identifiable health information.

The HIPAA Privacy Rule (Standards for Privacy of Individually Identifiable Health Information) (*3*) provides the first national standards for protecting the privacy of health information. The Privacy Rule regulates how certain entities, called covered entities, use and disclose certain individually identifiable health information, called protected health information (PHI). PHI is individually identifiable health information that is transmitted or maintained in any form or medium (e.g., electronic, paper, or oral), but excludes certain educational records and employment records. Among other provisions, the Privacy Rule

- gives patients more control over their health information;
- sets boundaries on the use and release of health records;
- establishes appropriate safeguards that the majority of health-care providers and others must achieve to protect the privacy of health information;
- holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights;
- strikes a balance when public health responsibilities support disclosure of certain forms of data;
- enables patients to make informed choices based on how individual health information may be used;
- enables patients to find out how their information may be used and what disclosures of their information have been made;
- generally limits release of information to the minimum reasonably needed for the purpose of the disclosure;
- generally gives patients the right to obtain a copy of their own health records and request corrections; and
- empowers individuals to control certain uses and disclosures of their health information.

The deadline to comply with the Privacy Rule is April 14, 2003, for the majority of the three types of covered entities specified by the rule [45 CFR § 160.102]. The covered entities are

- health plans,
- health-care clearinghouses, and
- health-care providers who transmit health information in electronic form in connection with certain transactions.

At DHHS, the Office for Civil Rights (OCR) has oversight and enforcement responsibilities for the Privacy Rule. Comprehensive guidance and OCR answers to hundreds of questions are available at http://www.hhs.gov/ocr/hipaa (*4*).

Impact on Public Health

Public health practice and research, including such traditional public health activities as program operations, public health surveillance, program evaluation, terrorism preparedness, outbreak investigations, direct health services, and public health research, use PHI to identify, monitor, and respond to disease, death, and disability among populations. Public health authorities have a long history of protecting and preserving the confidentiality of individually identifiable health information. They also recognize the importance of protecting individual privacy and respecting individual dignity to maintaining the quality and integrity of health data. CDC and others have worked to consistently strengthen federal and state public health information privacy practices and legal protections (*5*).

DHHS recognized the importance of sharing PHI to accomplish essential public health objectives and to meet certain other societal needs (e.g., administration of justice and law enforcement). Therefore, the Privacy Rule expressly permits PHI to be shared for specified public health purposes. For example, covered entities may disclose PHI, without individual authorization, to a public health authority legally authorized to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability [45 CFR § 164.512(b)] (Box 1). Further, the Privacy Rule permits covered entities to make disclosures that are required by other laws, including laws that require disclosures for public health purposes.

Thus, the Privacy Rule provides for the continued functioning of the U.S public health system. Covered entities should become fully aware of the scope of permissible disclosures for public health activities as well as state and local reporting laws and regulations. Moreover, a public health authority may also be a covered entity. For example, a public health agency that operates a health clinic, providing essential health-care services and performing covered transactions electronically, is a covered entity.

This report provides guidance to public health authorities and their authorized agents, researchers, and health-care providers in interpreting the Privacy Rule as it affects public health. CDC recommends that public health authorities share the information in this report with covered health-care providers and other covered entities and work closely with those entities to ensure implementation of the rule consistent with its intent to protect privacy while permitting authorized public health activities to continue.

Overview of the Privacy Rule

Who Is Covered

The authority of DHHS to issue health-information privacy regulations was limited by Congress in HIPAA to a defined set of covered entities. More complete definitions of these, and other terms, are located elsewhere in this report (Appendix A). Covered entities are as follows:

- Health plans. An individual or group plan that provides, or pays the cost of, medical care that includes the diagnosis, cure, mitigation, treatment, or prevention of disease. Health plans include private entities (e.g., health insurers and managed care organizations) and government organizations (e.g., Medicaid, Medicare, and the Veterans Health Administration).
- Health-care clearinghouses. A public or private entity, including a billing service, repricing company, or community health information system, that processes nonstandard data or transactions received from another entity into standard transactions or data elements, or vice versa.
- Health-care providers. A provider of health-care services and any other person or organization that furnishes, bills, or is paid for health care in the normal course of business. Health-care providers (e.g., physicians, hospitals, and clinics) are covered entities if they transmit health information in electronic form in connection with a transaction for which a HIPAA standard has been adopted by DHHS.

The Privacy Rule also establishes requirements for covered entities with regard to their nonemployee business associates (e.g., lawyers, accountants, billing companies, and other contractors) whose relationship with covered entities requires sharing of PHI. The Privacy Rule allows a covered provider or health plan to disclose PHI to a business associate if satisfactory written assurance is obtained that the business associate will use the information only for the purposes for which it was engaged, will safeguard the information from misuse, and will help the covered entity comply with certain of its duties under the Privacy Rule.

The Privacy Rule does not apply to all persons or entities that regularly use, disclose, or store individually identifiable health information. For example, the Privacy Rule does not cover employers, certain insurers (e.g., auto, life, and worker compensation), or those public agencies that deliver social security or welfare benefits, when functioning solely in these capacities.

Types of Health Information

Protected Health Information

The Privacy Rule protects certain information that covered entities use and disclose. This information is called protected health information (PHI), which is generally individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to 1) the past, present, or future physical or mental health, or condition of an individual; 2) provision of health care to an individual; or 3) payment for the provision of health care to an individual. If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered individually identifiable health information.

De-Identified Information

De-identified data (e.g., aggregate statistical data or data stripped of individual identifiers) require no individual privacy protections and are not covered by the Privacy Rule. De-identifying can be conducted through

- statistical de-identification --- a properly qualified statistician using accepted analytic techniques concludes the risk is substantially limited that the information might be used, alone or in combination with other reasonably available information, to identify the subject of the information [45 CFR § 164.514(b)]; or the
- safe-harbor method --- a covered entity or its business associate de-identifies information by removing 18 identifiers (Box 2) and the covered entity does not have actual knowledge that the remaining information can be used alone or in combination with other data to identify the subject [45 CFR § 164.514(b)].

In certain instances, working with de-identified data may have limited value to clinical research and other activities. When that is the case, a limited data set may be useful.

Limited Data Sets

Health information in a limited data set is not directly identifiable, but may contain more identifiers than de-identified data that has been stripped of the 18 identifiers [45 CFR § 164.514] (Box 3). A data-use agreement must establish who is permitted to use or receive the limited data set, and provide that the recipient will

- not use or disclose the information other than as permitted by the agreement or as otherwise required by law;
- use appropriate safeguards to prevent uses or disclosures of the information that are inconsistent with the data-use agreement;
- report to the covered entity any use or disclosure of the information, in violation of the agreement, of which it becomes aware;
- ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- not attempt to re-identify the information or contact the individual.

What is Required

For covered entities using or disclosing PHI, the Privacy Rule establishes a range of health-information privacy requirements and standards that attempt to balance individual privacy interests with the community need to use such data [45 CFR § 164.504]. Among its provisions, the Privacy Rule requires covered entities to

- notify individuals regarding their privacy rights and how their PHI is used or disclosed;
- adopt and implement internal privacy policies and procedures;

- train employees to understand these privacy policies and procedures as appropriate for their functions within the covered entity;
- designate individuals who are responsible for implementing privacy policies and procedures, and who will receive privacy-related complaints;
- establish privacy requirements in contracts with business associates that perform covered functions;
- have in place appropriate administrative, technical, and physical safeguards to protect the privacy of health information; and
- meet obligations with respect to health consumers exercising their rights under the Privacy Rule.

With respect to individuals, they are vested with the following rights:

- Receive access to PHI. Individual rights include inspections of records and the provision for copies of PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set, except for psychotherapy notes, information complied for use in civil, criminal, or administrative actions, and PHI maintained by a covered entity subject to the Clinical Laboratory Improvement Amendments of 1988 [42 CFR § 263(a)]. In the majority of cases, covered entities must accommodate a request or provide a process of denial, subject to review [45 CFR § 164.524].
- Request amendments to PHI. Individuals can request that covered entities amend PHI about the individual in a designated record set for as long as the PHI is maintained in a designated record set. If the covered entity agrees to the amendment, it must 1) identify the records affected; 2) append or provide a link to the amendment; 3) inform the individual the amendment has been made; and 4) work with other covered entities or business associates who possess or receive the data to make the amendments [45 CFR § 164.526]. If the covered entity denies this request, the Privacy Rule provides a process for contesting the denial [45 CFR § 164.526].
- Receive adequate notice. With limited exceptions, individuals have the right to receive a notice of the uses and disclosures the covered entity will make of their PHI, their rights under the Privacy Rule, and the covered entity's obligations with respect to that information. In certain cases, notice may be provided electronically. The notice must be in plain language (e.g., "your health information may be shared with public health authorities for public health purposes . . .") and posted where it is likely to be seen by patients [45 CFR § 164.520].
- Receive an accounting of disclosures. Upon request, covered entities are required to provide individuals with an accounting for certain types of disclosures of PHI, although the rule contains certain exceptions, including disclosures with individual authorization, disclosures related to providers' treatment, payment and health-care operations (TPO), and other exceptions. A typical a ccounting includes the name of the person or entity who received the information, date of the disclosure, a brief description of the information disclosed, and a brief e xplanation of the reasons for disclosure or copy of the request [45 CFR § 164.528]. However, requirements for accounting of public health disclosures may vary (see Accounting for Public Health Disclosures).
- Request restrictions. Individuals have the right to request a restriction on certain uses or disclosures of their PHI; however, the covered entity is not obligated to agree to such a request. If the covered entity does agree to a restriction, it must generally abide by the agreement, except for emergency treatment situations. But such an agreement is not effective to prevent certain permitted uses or disclosures [CFR 45 § 164.512].

Required PHI Disclosures

A covered entity is required by the Privacy Rule to disclose PHI in only two instances: 1) when an individual has a right to access an accounting of his or her PHI (see previous paragraph); and 2) when DHHS needs PHI to determine compliance with the Privacy Rule [45 CFR § 164.502(a)(2)]. Certain other uses and disclosures of PHI may be permitted without authorization, but are not required by the Privacy Rule. However, other federal, tribal, state, or local laws may compel disclosure.

Permitted PHI Disclosures Without Authorization

The Privacy Rule permits a covered entity to use and disclose PHI, with certain limits and protections, for TPO activities [45 CFR § 164.506]. Certain other permitted uses and disclosures for which authorization is not required follow. Additional requirements and conditions apply to these disclosures. The Privacy Rule text and OCR guidance should be consulted for a full understanding of the following:

- Required by law. Disclosures of PHI are permitted when required by other laws, whether federal, tribal, state, or local.
- Public health. PHI can be disclosed to public health authorities and their authorized agents for public health purposes including but not limited to public health surveillance, investigations, and interventions.
- Health research. A covered entity can use or disclose PHI for research without authorization under certain conditions, including 1) if it obtains documentation of a waiver from an institutional review board (IRB) or a privacy board, according to a series of considerations; 2) for activities preparatory to research; and 3) for research on a decedent's information.
- Abuse, neglect, or domestic violence. PHI may be disclosed to report abuse, neglect, or domestic violence under specified circumstances.
- Law enforcement. Covered entities may, under specified conditions, disclose PHI to law enforcement officials pursuant to a court order, subpoena, or other legal order, to help identify and locate a suspect, fugitive, or missing person; to provide information related to a victim of a crime or a death that may have resulted from a crime, or to report a crime.
- Judicial and administrative proceedings. A covered entity may disclose PHI in the course of a judicial or administrative proceeding under specified circumstances.
- Cadaveric organ, eye, or tissue donation purposes. Organ-procurement agencies may use PHI for the purposes of facilitating transplant.
- Oversight. Covered entities may usually disclose PHI to a health oversight agency for oversight activities authorized by law.
- Worker's compensation. The Privacy Rule permits disclosure of work-related health information as authorized by, and to the extent necessary to comply with, workers' compensation programs.

Other Authorized Disclosures

A valid authorization is required for any use or disclosure of PHI that is not required or otherwise permitted without authorization by the Privacy Rule. In general, these authorizations must

- specifically identify the PHI to be used or disclosed;
- provide the names of persons or organizations, or classes of persons or organizations, who will receive, use, or disclose the PHI;
- state the purpose for each request;
- notify individuals of their right to refuse to sign the authorization without negative consequences to treatment, payment, or health plan enrollment or benefit eligibility, except under specific circumstances;
- be signed and dated by the individual or the individual's personal representative;
- be written in plain language;
- include an expiration date or event;
- notify the individual of the right to revoke authorization at any time in writing, and how to exercise that right, and any applicable exceptions to that right under the Privacy Rule; and
- explain the potential for the information to be subject to redisclosure by recipient and no longer protected by the Privacy Rule.

The Privacy Rule and Public Health

The Privacy Rule recognizes 1) the legitimate need for public health authorities and others responsible for ensuring the public's health and safety to have access to PHI to conduct their missions; and 2) the importance of public health reporting by covered entities to identify threats to the public and individuals.

Accordingly, the rule 1) permits PHI disclosures without a written patient authorization for specified public health purposes to public health authorities legally authorized to collect and receive the information for such purposes, and 2) permits disclosures that are required by state and local public health or other laws. However, because the Privacy Rule affects the traditional ways PHI is used and exchanged among covered entities (e.g., doctors, hospitals, and health insurers), it can affect public health practice and research in multiple ways. To prevent misconceptions, understanding the Privacy Rule is important for public health practice. Some illustrative examples are presented in this report (Box 4). Also provided are sample letters that might prove useful in clarifying relationships involving public health and the Privacy Rule (Appendix B).

A public health authority is broadly defined as including agencies or authorities of the United States, states, territories, political subdivisions of states or territories, American Indian tribes, or an individual or entity acting under a grant of authority from such agencies and responsible for public health matters as part of an official mandate. Public health authorities include federal public health agencies (e.g., CDC, National Institutes of Health [NIH], Health Resources and Services Administration [HRSA], Substance Abuse and Mental Health Services Administration [SAMHSA], Food and Drug Administration [FDA], or Occupational Safety and Health Administration [OSHA]); tribal health agencies; state public health agencies (e.g., public health departments or divisions, state cancer registries, and vital statistics departments); local public health agencies; and anyone performing public health functions under a grant of authority from a public health agency [45 CFR § 164.501].

Public health agencies often conduct their authorized public health activities with other entities by using different mechanisms (e.g., contracts and memoranda or letters of agreement). These other entities are public health authorities under the Privacy Rule with respect to the activities they conduct under a grant of authority from such a public health agency. A covered entity may disclose PHI to public health authorities and to these designated entities pursuant to the public health provisions of the Privacy Rule.

The Privacy Rule permits covered entities to disclose PHI, without authorization, to public health authorities or other entities who are legally authorized to receive such reports for the purpose of preventing or controlling disease, injury, or disability. This includes the reporting of disease or injury; reporting vital events (e.g., births or deaths); conducting public health surveillance, investigations, or interventions; reporting child abuse and neglect; and monitoring adverse outcomes related to food (including dietary supplements), drugs, biological products, and medical devices [45 CFR 164.512(b)]. Covered entities may report adverse events related to FDA-regulated products or activities to public agencies and private entities that are subject to FDA jurisdiction [45 CFR 164.512(b)(1)(iii)]. To protect the health of the public, public health authorities might need to obtain information related to the individuals affected by a disease. In certain cases, they might need to contact those affected to determine the cause of the disease to allow for actions to prevent further illness. Also, covered entities may, at the direction of a public health authority, disclose protected health information to a foreign government agency that is acting in collaboration with a public health authority [45 CFR 164.512(b)(1)(i)].

To receive PHI for public health purposes, public health authorities should be prepared to verify their status and identity as public health authorities under the Privacy Rule. To verify its identity, an agency could provide any one of the following:

- if the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
- if the request is in writing, the request is on the appropriate government letterhead;
- if the disclosure is to a person acting on behalf of a public health authority, a written statement on appropriate government letterhead that the person is acting under the government's authority [45 CFR § 164.514(h)(2)].

Public health authorities receiving information from covered entities as required or authorized by law [45 CFR 164.512(a)] [45 CFR 164.512(b)] are not business associates of the covered entities and therefore are

not required to enter into business associate agreements. Public health authorities that are not covered entities also are not required to enter into business associate agreements with their public health partners and contractors. Also, after PHI is disclosed to a public health authority pursuant to the Privacy Rule, the public health authority (if it is not a covered entity) may maintain, use, and disclose the data consistent with the laws, regulations, and policies applicable to the public health authority.

Disclosures for Public Health Purposes

The Privacy Rule allows covered entities to disclose PHI to public health authorities when required by federal, tribal, state, or local laws [45 CFR 164.512(a)]. This includes state laws (or state procedures established under such law) that provide for receiving reporting of disease or injury, child abuse, birth, or death, or conducting public health surveillance, investigation, or intervention.

For disclosures not required by law, covered entities may still disclose, without authorization, to a public health authority authorized by law to collect or receive the information for the purpose of preventing or controlling disease, injury, or disability, the minimum necessary information to accomplish the intended public health purpose of the disclosure [45 CFR 164.512 (b)] (Box 1).

For example, to protect the health of the public, public health officials might need to obtain information related to persons affected by a disease. In certain cases, they might need to contact those affected to determine the cause of the disease to allow for actions to prevent further illness. The Privacy Rule continues to allow for the existing practice of sharing PHI with public health authorities who are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public. Examples of such activities include those directed at the reporting of disease or injury, reporting adverse events, reporting births and deaths, and investigating the occurrence and cause of injury and disease (*1*).

Although it is not a defined term, DHHS interpreted the phrase "authorized by law" to mean that a legal basis exists for the activity. Further, DHHS called the phrase "a term of art," including both actions that are permitted and actions that are required by law [64 FR 59929, November 3, 1999]. This does not mean a public health authority at the federal, tribal, state, or local level must have multiple disease or condition-specific laws that authorize each collection of information. Public health authorities operate under broad mandates to protect the health of their constituent populations.

Requirements for Covered Entities

Accounting for Public Health Disclosures

Although the Privacy Rule permits disclosures of PHI to public health authorities, covered entities must comply with certain requirements related to these disclosures. One such requirement is that a covered entity must be able to provide an individual, upon request, with an accounting of certain disclosures of PHI. The covered entity is not required to account for all disclosures of PHI. For example, an accounting is not required for disclosures made

- prior to the covered entity's compliance date;
- for TPO purposes;
- to the individual or pursuant to the individual's written authorization; or
- as part of a limited data set.

However, usually an accounting is required for disclosures made without authorization, including public health purposes.

The required accounting for disclosures may be accomplished in different ways. Typically, the covered entity must provide the individual with an accounting of each disclosure by date, the PHI disclosed, the identity of the recipient of the PHI, and the purpose of the disclosure. However, where the covered entity

has, during the accounting period, made multiple disclosures to the same recipient for the same purpose, the Privacy Rule provides for a simplified means of accounting. In such cases, the covered entity need only identify the recipient of such repetitive disclosures, the purpose of the disclosure, and describe the PHI routinely disclosed. The date of each disclosure need not be tracked. Rather, the accounting may include the date of the first and last such disclosure during the accounting period, and a description of the frequency or periodicity of such disclosures. For example, the vast amount of data exchanged between covered entities and public health authorities is made through ongoing, regular reporting or inspection requirements. A covered health-care provider may routinely report all cases of measles it diagnoses to the local public health authority. An accounting of such disclosures to a requesting individual would need to identify the local public health authority receiving the PHI, the PHI disclosed, the purpose of the disclosure (required for communicable disease surveillance), the periodicity (weekly), and the first and last dates of such disclosures during the accounting period (May 1, 2003 to June 1, 2003). Thus, the covered entity would not need to annotate each patient's medical record whenever a routine public health disclosure was made.

Notice of Privacy Practices

With certain exceptions, under the Privacy Rule, individuals have the right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity, as well as their rights and the covered entity's legal obligations. Notices must be in plain language and clearly posted. Certain covered entities must make a good faith effort to obtain an individual's acknowledgment of receipt of this notice. In certain cases, notice may be provided electronically.

Minimum Necessary Standard

The Privacy Rule usually directs covered entities to limit the amount of information disclosed to the minimum necessary to achieve the specified goal [45 CFR § 164.514(d)(1)]. This requirement usually applies to disclosures to a public health agency. It would not apply, however, if the disclosure were required by law, authorized by the individual, or for treatment purposes. A covered entity may also reasonably rely on a public official's determination that the information requested is the minimum necessary for the public health purpose.

Public Health Authorities Performing Covered Functions

Public health authorities at the federal, tribal, state, or local levels that perform covered functions (e.g., providing health care or insuring individuals for health-care costs), may be subject to the Privacy Rule's provisions as covered entities. For example, a local public health authority that operates a health clinic providing essential health-care services to low-income persons and performs certain electronic transactions might be defined under the Privacy Rule as a covered health-care provider and therefore a covered entity. Flow charts and interactive tools designed to help determine covered entity status are provided online by the Centers for Medicare and Medicaid Services, available at http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp.

The following are examples of public health authority functions that make them covered entities:

- **Public health authorities as covered health-care providers.** A public health authority that conducts health care as part of its activities is a covered health-care provider if it also performs electronic transactions covered by the HIPAA Transactions Rule as part of these activities. The fact that these activities are conducted in pursuit of a public health goal (e.g., vaccinating children or screening a targeted population for sexually transmitted diseases) does not preclude the public health authority from being a covered entity.
- **Public health authorities as health plans.** Under the Privacy Rule, a health plan is an individual or group plan that provides, or pays the cost of, medical care. This specifically includes government health plans (e.g., Medicare, Medicaid, or Veterans Health Administration). However, the Privacy Rule defines health plan to exclude government-funded programs whose principal activity is the

direct provision of health care to persons or the making of grants to fund the direct provision of health care to persons [45 CFR § 160.103]. Examples include the Ryan White Comprehensive AIDS Resources Emergency Act. Although certain government programs that fund providers directly may not be health plans, government programs that reimburse providers or otherwise fund providers to perform direct health-care services should carefully analyze the details of their programs to determine if they are performing covered functions.

- **Public health authorities as health-care clearinghouses.** Although unlikely, a public health authority might be a health-care clearinghouse if it receives health information from another entity and translates that information from a nonstandard format into a standard transaction or standard data elements (or vice versa). Operators of community health information systems should carefully consider whether they meet the definition for a health-care clearinghouse.
- **Public health agencies as hybrid entities.** A public health agency that is a covered entity, and has both covered and noncovered functions may become a hybrid entity by designating its health-care components. By designating itself as a hybrid entity, a public health authority can carve out its noncovered functions, so that the majority of Privacy Rule provisions apply only to its health-care component, which is required to comply with the Privacy Rule requirements, including using and disclosing PHI only as authorized, meeting the administrative requirements, accounting for disclosure of PHI, and providing a notice of practices. However, such a designation does not preclude the public health authority from continuing to conduct authorized public health functions. A covered entity that is also a public health authority may use, as well as disclose, PHI for public health purposes to the same extent it would be permitted to disclose the PHI as a public health authority.

The Privacy Rule and Public Health Research

The topic of research under the Privacy Rule is covered in depth in the DHHS report, Protecting Personal Health Information in Research --- Understanding the HIPAA Privacy Rule (*6*). The Privacy Rule provides separate provisions for disclosure without individual authorization for public health purposes and for certain research [45 CFR § 164.512(b)] [45 CFR § 164.512(i)]. Other federal law pertaining to research stresses the importance of distinguishing between research and practice to ensure that human subjects are appropriately protected [45 CFR Part 46]. For certain activities, this distinction is not always clear. A full discussion of the distinctions between public health practice and research is beyond the scope of this document. However, CDC and others provide guidance in this area (*7--9*).

Research Versus Practice

The definition of research is the same for the Privacy Rule and the Common Rule (*10*) --- systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Research is designed to test a hypothesis, permit conclusions to be drawn, and thereby to develop or contribute to generalizable knowledge. The majority of public health activities (e.g., public health surveillance, and disease prevention and control projects) are based on scientific evidence and data collection or analytic methods similar to those used in research. However, they are not designed to contribute to generalizable knowledge. Their primary purpose is to protect the health of the population through such activities as disease surveillance, prevention, or control.

The Belmont Report (*11*) defines practice as interventions designed solely to enhance the well-being of a person, patient, or client, and which have reasonable expectation of success. The report further states that the purpose of medical or behavioral practice is to provide diagnosis, preventive treatment, or therapy to particular patients. For public health agencies, the patient is the community. Public health practice activities (e.g., public health surveillance, disease control, or program evaluation) are undertaken with the intent to benefit a specific community, although occasionally they may provide unintended generalizable benefits to others.

Some public health activities that are initially public health practice may subsequently evolve into a research activity (e.g., an investigation to determine the cause of an outbreak that incorporates a research

study evaluating the efficacy of a new drug to treat the illness). When that is the case, the disclosures may be made initially under the public health provisions of the Privacy Rule. But when the activity becomes an ongoing research activity, the entity should consider application of the relevant research disclosures provisions to continue to obtain information for this purpose. Moreover, there may be cases where the activity is both research and public health practice (e.g., an ongoing survey to monitor health conditions in the population, data from which can also be analyzed for research purposes). In those cases, disclosures may be made either under the research provisions or the public health provisions, as appropriate --- the covered entity need not comply with both sets of requirements.

The Privacy Rule and Other Laws

- **Federal laws.** Covered entities subject to the Privacy Rule are also subject to other federal statutes and regulations. The specific relationship of the Privacy Rule and certain federal laws is discussed in the preamble to the December 2000 Final Rule [65 Fed.Reg. 82481]. In certain instances, the Privacy Rule imposes requirements in direct conflict with other federal laws or regulations. In those instances, an analysis will be necessary to determine whether the later provision was intended to overrule the prior law or regulation.
- **State laws.** As a federal regulatory standard, the Privacy Rule preempts only those contrary state laws relating to the privacy of individually identifiable health information that have less stringent requirements or standards than the Privacy Rule (i.e., more stringent laws remain in effect). In addition, DHHS may, upon specific request from a state or other entity or person, determine that a provision of state law that is contrary to the federal requirements and that meets certain additional criteria, will not be preempted by the federal requirements. Thus, preemption of a contrary state law will not occur if the Secretary or designated DHHS official determines, in response to a request, that the state law 1) is necessary to prevent fraud and abuse related to the provision of or payment for health care; 2) is necessary to ensure appropriate state regulation of insurance and health plans to the extent expressly authorized by statute or regulation; 3) is necessary for state reporting on health-care delivery or costs; 4) is necessary to serve a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or 5) has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances. The Privacy Rule specifically does not preempt contrary state public health laws that provide for the reporting of disease or injury, child abuse, birth or death, or for the conduct of public health surveillance, investigation, or intervention [45 CFR § 160.202].

Online Resources

References to non-DHHS sites on the Internet are provided as a service to *MMWR* readers and do not constitute or imply endorsement of these organizations or their programs by CDC or the U.S. Department of Health and Human Services. CDC is not responsible for the content of these sites. URL addresses listed in *MMWR* were current as of the date of publication.

Federal Government Resources

DHHS Office for Civil Rights --- HIPAA guidelines
http://www.hhs.gov/ocr/hipaa

CDC --- Privacy Rule guidelines
http://www.cdc.gov/privacyrule

Centers for Medicare and Medicaid Services
http://www.cms.gov/hipaa/
http://www.cms.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

Health Resources and Services Administration --- HIPAA
http://www.hrsa.gov/website.htm

National Center for Health Statistics
http://www.cdc.gov/nchs/otheract/phdsc/phdsc.htm

National Committee on Vital and Health Statistics
http://www.ncvhs.hhs.gov/

National Health Information Infrastructure
http://www.health.gov/ncvhs-nhii/

Indian Health Service --- HIPAA
http://www.ihs.gov/AdminMngrResources/HIPAA/index.cfm

National Institutes of Health
http://privacyruleandresearch.nih.gov

Substance Abuse and Mental Health Services Administration --- HIPAA
http://www.samhsa.gov/hipaa/

State Government Resources

California
http://www.dhs.ca.gov/hipaa/
http://www.ohi.ca.gov/state/calohi/ohiHome.jsp
http://www.dmh.ca.gov/hipaa/

Colorado
http://www.cdphe.state.co.us/HIPAA/

Florida
http://www.myflorida.com/myflorida/sto/hipaa/

Illinois
http://www.state.il.us/dpa/hipaa.html

Kentucky
http://chs.state.ky.us/dms/HIPAA/default.htm
http://dmhmrs.chr.state.ky.us/hipaa.asp

Maryland
http://www.mhcc.state.md.us/edi/hipaa/_hipaa.htm
http://dhmh.state.md.us/HIPAA/

Minnesota
http://www.dhs.state.mn.us/hipaa/

Missouri
http://www.health.state.mo.us/HIPAA/

New York
http://www.oft.state.ny.us/hipaa/index.htm

North Carolina
http://dirm.state.nc.us/hipaa/

Ohio
http://www.state.oh.us/hipaa/

Pennsylvania
http://www.dpw.state.pa.us/omap/hipaa/omaphipaa.asp
http://www.insurance.state.pa.us/html/hipaa.html

South Carolina
http://www.hipaa.state.sc.us/

Texas
http://www.hhsc.state.tx.us/NDIS/NDISTaskForce.html

Virginia
http://www.dmas.state.va.us/hpa-home.htm

Wisconsin
http://www.dhfs.state.wi.us/HIPAA/

Associations, Nonprofit Organizations, and Academic Resources

American Hospital Association --- HIPAA
http://www.hospitalconnect.com/aha/key_issues/hipaa/resources/resources.html

American Medical Association --- HIPAA
http://www.ama-assn.org/ama/pub/category/4234.html

Association of State and Territorial Health Officials --- HIPAA
http://www.astho.org/?template=hipaa.html

Georgetown University Health Privacy Project
http://www.healthprivacy.org/

Joint Healthcare Information Technology Alliance
http://www.jhita.org/

National Association of Health Data Organizations
http://www.nahdo.org/

National Association of Insurance Commissioners
http://www.naic.org/1privacy/initiatives/health_privacy.htm

National Governors Association --- HIPAA
http://www.nga.org/center/topics/1,1188,C_CENTER_ISSUE^D_4324,00.html

North Carolina Healthcare Information and Communications Alliance
http://www.nchica.org/

Public Health Grand Rounds HIPAA Privacy Rule: Enhancing or Harming Public Health?
http://www.publichealthgrandrounds.unc.edu/

Stanford University Medical School --- HIPAA
http://www.med.stanford.edu/HIPAA/

Workgroup for Electronic Data Interchange --- Strategic National Implementation Process
http://www.wedi.org/snip/

Acknowledgments

This report was prepared by Salvatore Lucido, M.P.A., and Denise Koo, M.D., Office of the Associate Director for Science, Epidemiology Program Office, CDC, in collaboration with James G. Hodge, Jr., J.D., Center for Law and the Public's Health, Georgetown and Johns Hopkins Universities, Baltimore, Maryland. The preparers are grateful for the participation of Deborah Tress, J.D., Kenya Ford, J.D., and Heather Horton, J.D., Office of the General Counsel, Department of Health and Human Services, CDC/ATSDR Branch; the CDC Working Group on the Privacy Rule; and Beverly Dozier, J.D., Lance A. Gable, J.D., Lawrence O. Gostin, J.D., Gail Horlick, J.D., and Jennifer Kurle.

The preparers also thank the following partners for their valuable input: Association of State and Territorial Health Officers, Council of State and Territorial Epidemiologists, National Association of County and City Health Officials, National Association of Health Data Organizations, Association of Public Health Laboratories, and National Association for Public Health Statistics and Information Systems.

References

1. Gostin LO, Hodge JG Jr. Personal privacy and common goods: a framework. Minnesota Law Review 2002;86:1439--80.
2. Health Insurance Portability and Accountability Act of 1996. Pub. L. No. 104-191, 110 Stat. 1936 (1996).
3. Office for Civil Rights, Department of Health and Human Services. Title 45 of the Code of Federal Regulations Parts 160 and 164. Available at http://www.dhhs.gov/ocr/combinedregtext.pdf.
4. Office for Civil Rights. OCR guidance explaining significant aspects of the Privacy Rule, 2002. Department of Health and Human Services. Available at http://www.hhs.gov/ocr/hipaa.
5. Gostin, LO, Hodge JG Jr. Privacy Law Advisory Committee. Model state public health information privacy act, 1999. Available at http://www.publichealthlaw.net/Resources/ResourcesPDFs/modelprivact.pdf.
6. Department of Health and Human Services. Protecting personal health information in research --- understanding the HIPAA Privacy Rule. Department of Health and Human Services. Washington, D.C.: 2003 (in press).
7. Snider DE, Stroup DF. Defining research when it comes to public health. Public Health Rep 1997:112:29--32.
8. CDC. Guidelines for defining public health research and public health nonresearch. Available at http://www.cdc.gov/od/ads/opspoll1.htm.
9. Amoroso PJ, Middaugh JP. Research vs. public health practice: when does a study require IRB review? Prev Med 2003;36:250--3.
10. Office for Protection from Research Risks, National Institutes of Health, Department of Health and Human Services. Public welfare: protection of human subjects, 2001. [45 CFR 46]. Available at http://ohrp.osophs.dhhs.gov/humansubjects/guidance/45cfr46.htm.
11. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Belmont report: ethical principles and guidelines for the protection of human subjects of research. Department of Health, Education and Welfare. Available at http://www.med.umich.edu/irbmed/ethics/belmont/BELMONTR.HTM.

* Prepared by CDC staff, in consultation with the Office of the General Counsel, the Office for Civil Rights, other offices and agencies within the U.S. Department of Health and Human Services, Washington, D.C., and health privacy specialists.

Box 1

BOX 1. Protected health information (PHI) disclosures by covered entities for public health activities requiring no authorization under the Privacy Rule

Without individual authorization, a covered entity may disclose PHI to a public health authority* that is legally authorized to collect or receive the information for the purposes of preventing or controlling disease, injury, or disability including, but not limited to

- reporting of disease, injury, and vital events (e.g., birth or death); and
- conducting public health surveillance, investigations, and interventions.

PHI may also be disclosed without individual authorization to

- report child abuse or neglect to a public health or other government authority legally authorized to receive such reports;
- a person subject to jurisdiction of the Food and Drug Administration (FDA) concerning the quality, safety, or effectiveness of an FDA-related product or activity for which that person has responsibility;
- a person who may have been exposed to a communicable disease or may be at risk for contracting or spreading a disease or condition, when legally authorized to notify the person as necessary to conduct a public health intervention or investigation; and
- an individual's employer, under certain circumstances and conditions, as needed for the employer to meet the requirements of the Occupational Safety and Health Administration, Mine Safety and Health Administration, or a similar state law.

Source: Adapted from [45 CFR § 164.512(b)].

* Or to an entity working under a grant of authority from a public health authority, or when directed by a public health authority, to a foreign government agency that is acting in collaboration with a public health authority.

Return to top.

Box 2

BOX 2. Individual identifiers under the Privacy Rule

The following 18 identifiers of a person, or of relatives, employers, or household members of a person must be removed, and the covered entity must not have actual knowledge that the information could be used alone or in combination with other information to identify the individual, for the information to be considered de-identified and not protected health information (PHI):

- names;
- all geographic subdivisions smaller than a state, including county, city, street address, precinct, zip code,* and their equivalent geocodes;
- all elements of dates (except year) directly related to an individual; all ages >89 and all elements of dates (including year) indicative of such age (except for an aggregate into a single category of age >90);
- telephone numbers;
- fax numbers;
- electronic mail addresses;
- Social Security numbers;
- medical record numbers;
- health-plan beneficiary numbers;
- account numbers;
- certificate and license numbers;
- vehicle identifiers and serial numbers, including license plate numbers;
- medical device identifiers and serial numbers;
- Internet universal resource locators (URLs);
- Internet protocol (IP) addresses;
- biometric identifiers including fingerprints and voice prints;
- full-face photographic images and any comparable images; and
- any other unique identifying number, characteristic, or code, except that covered identities may, under certain circumstances, assign a code or other means of record identification that allows de-identified information to be re-identified.

Source: Adapted from §45 CFR § 164.514(b)(2)(i).

* The first three digits of a zip code are excluded from the PHI list if the geographic unit formed by combining all zip codes with the same first three digits contains >20,000 persons.

Return to top.

Box 3

BOX 3. Use of limited data sets under the Privacy Rule

The following protected health information (PHI) can be included, without authorization, in a limited data set for public health, research, or health-care operations:

- town or city, state, and zip code; and
- elements of dates related to a person (e.g., years, birth dates, admission dates, discharge dates, and dates of death).

To disclose a limited data set, a covered entity must enter into a data-use agreement with the recipient, which agrees to use or disclose the PHI for limited purposes. Disclosure of a limited data set is not subject to the accounting requirement, but must meet the minimum necessary standards of the Privacy Rule.

Return to top.

Box 4

BOX 4. Examples of situations related to the Privacy Rule and public health

State cancer registry. Under a state law, health-care providers are required to report cancer cases to a state's cancer registry. Names are included to prevent duplicate reporting and counting. State law protects the confidentiality of the data. Can covered entities disclose the information under the Privacy Rule?

Privacy Rule effect. Covered entities may disclose PHI to a public health agency, or any other entity, when the disclosure is required by law. However, as covered entities, the providers must give an accounting to the persons whose PHI has been shared. The state agency may use and further disclose the PHI consistent with applicable state law.

State university-maintained cancer registry. Under a state law, health-care providers are mandated to report cancer cases to a state health department's cancer registry. The state health department contracts with a state university to receive the reports and maintain its registry. As covered entities, can health-care providers disclose PHI to the state university under the Privacy Rule?

Privacy Rule effect. As noted in the previous example, covered entities may disclose, without authorization, PHI to the cancer registry under the Privacy Rule, which expressly permits disclosure of PHI as required by law and sharing of PHI with public health authorities for public health purposes. The state university is acting under a grant of authority from a public health authority, the state health department. The university can use and disclose the information, without authorization, consistent with its agreement with the state health department and applicable state law.

Early hearing detection and intervention. An early hearing detection and intervention program in a state needs data from two large hospitals. The state does not have a law requiring reporting of hearing loss. Under the Privacy Rule, can covered entities release results of newborn hearing-screening tests to the state program?

Privacy Rule effect. The Privacy Rule expressly permits release of PHI, without authorization, from a covered entity to a public health authority (e.g., the state health department), which is authorized by law to receive PHI for the purpose of controlling disease, injury, or disability. The rule does not require a state law mandating such disclosures for PHI to be released to a public health authority. Finally, the covered entities may rely upon the state's representation that the information requested is the minimum necessary for the purposes of the registry.

Disease registry maintained by private foundation. A private foundation maintains a disease registry as a way to support research and service for those with the disease. Can health-care providers release PHI to the foundation under the Privacy Rule?

Privacy Rule effect. Nongovernment disease registries (e.g., those maintained by foundations and other private organizations) are not considered public health authorities unless they have a grant of authority from a public health authority. With such a grant, covered entities may disclose PHI to the foundations. But without a grant of authority, PHI may be released only under one of the following situations:

- Release is authorized by the patient.
- The PHI is de-identified.
- The PHI is contained in a limited data set governed by a data-use agreement.
- Release of PHI is in accord with the rule's provisions for disclosure for research without authorization.
- Release is otherwise permitted by the rule (e.g., to entities subject to the jurisdiction of the Food and Drug Administration (FDA) [45 CFR § 164.512(b)(1)(iii)]).

Surveillance project. A state health department that is not a covered entity conducts a surveillance project on human immunodeficiency virus (HIV) and acquired immunodeficiency syndrome (AIDS). The HIV/AIDS surveillance project is an interview study. It asks for self-reported information from participants, including dates of diagnosis and visits for care. Is this PHI covered by the Privacy Rule?

Privacy Rule effect. Information collected directly from persons by a person, agency, or institution that is not a covered entity, including individually identifiable information, is not covered by the Privacy Rule.

Return to top.

Use of trade names and commercial sources is for identification only and does not imply endorsement by the U.S. Department of Health and Human Services.

References to non-CDC sites on the Internet are provided as a service to *MMWR* readers and do not constitute or imply endorsement of these organizations or their programs by CDC or the U.S. Department of Health and Human Services. CDC is not responsible for the content of pages found at these sites. URL addresses listed in *MMWR* were current as of the date of publication.

Disclaimer All *MMWR* HTML versions of articles are electronic conversions from ASCII text into HTML. This conversion may have resulted in character translation or format errors in the HTML version. Users should not rely on this HTML document, but are referred to the electronic PDF version and/or the original *MMWR* paper copy for the official text, figures, and tables. An original paper copy of this issue can be obtained from the Superintendent of Documents, U.S. Government Printing Office (GPO), Washington, DC 20402-9371; telephone: (202) 512-1800. Contact GPO for current prices.

**Questions or messages regarding errors in formatting should be addressed to mmwrq@cdc.gov.

Page converted: 4/11/2003

SAFER·HEALTHIER·PEOPLE™
Morbidity and Mortality Weekly Report
Centers for Disease Control and Prevention
1600 Clifton Rd, MailStop E-90, Atlanta, GA 30333,
U.S.A

This page last reviewed 4/11/2003

EXHIBIT 6

Skip Navigation

U.S. Department of Health & Human Services

Improving the health, safety, and well-being of America

Health Information Privacy

To provide individuals with an accounting for disclosures, does a covered entity have to document each medical record that may be accessed by a public health authority in the course of surveillance activities that involve all patient records?

Answer:

The Privacy Rule does not require a notation in each medical record that has been accessed by public health authorities, as long as the information required under the Privacy Rule is included in the accounting for disclosures. Where, as with many public health disclosures, access to an entire universe of records is involved, tracking disclosures can be accomplished without the need for documentation in each record. This flexibility in the manner of documentation facilitates complying with the accounting requirement.

By way of background, a covered entity may disclose protected health information (PHI) without the patient's authorization to a public health authority that is legally permitted to collect or receive such information for public health surveillance or related activities (45 CFR 164.512(b)(1)). A covered entity is also required by the Privacy Rule to account to the patient for such disclosures of PHI, if the patient asks (45 CFR 164.528). Further, under the Privacy Rule, making a set of records available for review by a third party constitutes a "disclosure" of the PHI in the entire set of records, regardless of whether the third party actually reviews any particular record. See 45 CFR 164.501, for the definition of disclosure. Thus, mere access by a third party, such as a public health authority, to PHI is a disclosure and subject to an accounting for disclosures.

Public health surveillance activities often involve a retrospective review by a public health authority of a universe of patient records to identify reportable events. When a reportable case is identified, the specific data items pertinent to the public health surveillance activity are extracted and reported to the public health authority.

For example, retrospective review of the medical charts for all patients treated by a health care provider or all charts of patients treated in the entity's emergency department may be required to identify cases of new or previously unknown infectious agents, clinical conditions associated with the use or abuse of illicit or prescription drugs, or adverse events or reactions associated with pharmaceuticals or medical devices. In these cases, as noted above, all records to which access was provided to the public health authority are deemed to have been disclosed under the Privacy Rule. Because of the universal nature of the access provided, the documentation required for the disclosure can be easily maintained. The covered entity need only document the identity (and address if known) of the public health authority to which access was provided, a description of the records and PHI subject to access, the purpose for the disclosure, and when access was provided. This documentation need not be noted in each record. It would be sufficient, for instance, for the covered entity to maintain a separate notation of such disclosures, applicable to all records so accessed. Then, if an individual requests an accounting, the covered entity need only determine whether the individual's records were among the universe of records to which the public health authority was granted access. All individuals whose records were accessed in this fashion would receive the same accounting for the disclosure.

For example, if on August 1, 2003, a hospital began providing a public health authority ongoing access to the medical charts of all patients treated in its emergency department to identify reportable cases and extract relevant information required for a particular surveillance activity, it would be sufficient, under §164.528(b)(2), for the accounting to include the following:

- the identity, and address, if known, of the public health authority;
- a statement that the public health authority had access to medical charts for patients treated in the emergency department
- the date (or approximate range of dates) when the individual's record was subject to access (e.g., access provided within a week of treatment in ER on [fill in date of individual visit]); and
- a statement of the purpose of the access (e.g., identify the particular public health surveillance activity).

The same basic statement could then be provided in response to a request for an accounting by any individual who was seen in the emergency department of the hospital on or after August 1, 2003.

Date Created: 08/28/2003
Last Updated: 11/06/2006

EXHIBIT 7

HIV/AIDS Care toolbox for HIV/AIDS Care

Selection and Implementation of Health IT Tools for HIV/AIDS Care

Financing Health IT

Improving Quality and Efficiency with Health IT for HIV/AIDS Care

Security and Privacy Issues

Share

How Do I Ensure Security in Our System?

Ensuring the security of protected health information (PHI) in your health IT system requires that you institute measures to guard against unauthorized use and disclosure of PHI. The HIPAA Standards for the Protection of Electronic Protected Health Information, known as the Security Rule, applies only to PHI in electronic form. As with the Privacy Rule, the Security Rule requires covered entities to have contracts or other arrangements in place with their business associates to ensure that the business associates will appropriately safeguard the electronic PHI.

Below are descriptions and overviews of the administrative, physical, and technical safeguards required for the security of PHI when using electronic health IT. These are discussed in detail in the Privacy and Security Module of the Health IT Adoption Toolbox.

Administrative Safeguards:

Administrative safeguards refer to the policies and procedures that exist in your practice to protect the security, privacy, and confidentiality of you patients' PHI. There are administrative safeguards that are required by both the HIPAA Privacy Rule and the HIPAA Security Rule. The administrative safeguards required under the HIPAA Security Rule include:

- Identifying relevant information systems
- Conducting a risk assessment
- Implementing a risk management program
- Acquiring IT systems and services
- Creating and deploying policies and procedures
- Developing and implementing a sanctions policy

Assessing the risk of unauthorized use or disclosure is an important step in your overall plan for maintaining security within your system and is especially important when treating patients with HIV/AIDS. The security risk assessment and risk management safeguards are discussed further in the response to the last question of this module, "How Do I Comply with Meaningful Use Requirements?"

Physical Safeguards:

Physical safeguards for PHI and health IT refer to measures to protect the hardware and the facilities that store PHI. Physical threats, whether in electronic or paper formation, affect the security of health information. Some of the safeguards for electronic and paper-based systems are similar, but some safeguards are specific to health IT. Policies and procedures must be put in place to physically safeguard health IT. These elements include:

About

Health Information Technology Toolboxes help health centers, safety net providers, and ambulatory care providers with electronic and online resources and technical assistance to improve patient care. More>

Stay Informed

Register for the HealthIT and Quality Improvement eNewsletter

Comments?
E-mail the HealthIT e-mail box:
healthit@hrsa.gov

- **Facility access controls** – Limitations for physical access to the facilities where health IT is housed, while ensuring authorized personnel are allowed access.
- **Workstation use** – Specifications for the appropriate use of workstations and the characteristics of the physical environment of workstations that can access PHI.
- **Workstation security** – Restrictions on access to workstations with PHI.
- **Device and media controls** –Receipt and removal of hardware and electronic media that contain PHI into and out of the facility and the movement of these items within a covered entity, including disposal, reuse of media, accountability, and data backup and storage.

Technical Safeguards:

Technical safeguards are safeguards that are built into your health IT system to protect health information and to control access to it. This includes measures to limit access to electronic information, to encrypt and decrypt electronic information, and to guard against unauthorized access to that information while it is being transmitted to others. Procedures and policies are required to address the following elements of technical safeguards:

- **Access control** - Allowing only access to persons or software programs that have appropriate access rights to data or PHI by using, for example, unique user identification protocols, emergency access procedures, automatic logoff, and encryption and decryption mechanisms.
- **Audit controls** - Recording and examining activity in health IT systems that contain or use PHI.
- **Integrity** - Protecting PHI from improper alteration or destruction, including implementation of mechanisms to authenticate PHI.
- **Person or entity authentication** - Verifying that a person or entity seeking access to PHI is who or what they claim to be (proof of identity).
- **Transmission security** - Guarding against unauthorized access to PHI that is being transmitted over an electronic communications network.

Having technical safeguards in place can protect against various intended and unintended uses and disclosures of PHI. The table below provides examples of risks and technical safeguards. Some of these safeguards are preventive measures to protect PHI, while others ensure that you are made aware of any unauthorized uses or disclosures. Furthermore, you will need to conduct regular checks of your system so that you can see who accessed the PHI stored in your system and when it was accessed.

Risk	Technical Safeguard
PHI vulnerable to unauthorized disclosure, such as when PHI is left clearly visible on a computer screen after use	Ensure that computer locks and the screen disappears after a certain period of inactivity, and that only authorized users of that EHR can log back into the system.
PHI is exchanged with outside providers, reported to public health authorities, or moved to	Ensure that all data are encrypted and transferred over secure data communication lines.

other media such as portable drives or a personal laptop	Institute specific policies restricting the movement of HIV/AIDS related PHI to portable storage devices.
Health care workers, other than those who are authorized to view a patient's PHI, use the system to review the PHI to discover that patient's HIV/AIDS status	Require a password for access to PHI. Ensure that appropriate roles and role based access is defined and applied to staff. Conduct routine audit to see who has accessed sensitive data. Train all employees on the rules, regulations, and consequences of unauthorized access.
Health care workers, authorized to have access to a patient's PHI but not authorized to know the patient's HIV/AIDS status, inadvertently come across HIV/AIDS status when looking through the patient's EHR	Segregate HIV-related information into another section of the EHR that cannot be accessed unintentionally or intentionally by those without authorization. Ensure that role based access is configured and activated in the IT system. This would include any information related to HIV/AIDS status, such as test results, treatments, and participation in clinical trials or research.
Passwords are left in open areas, or passwords become vulnerable to theft from outside sources seeking to acquire patient data illegally	Institute a system for user authentication. Examples include using additional security codes to log in, requiring answers to a set of questions before log in, or fingerprint or iris scanning technology. Adopt a clear policy on passwords and educate staff on the policy.

While these risks exist with both health IT and paper record systems, computer-based systems can have security features built into the software to protect against unauthorized use or disclosure. Many health IT systems have built-in security protections. Also, EHRs that are certified by ONC for Meaningful Use must meet ONC Standards and Certification Criteria. An EHR must meet nine security criteria to be certified for the first stage of Meaningful Use.

Below are the nine security protection capabilities required for EHR certification and the one optional capability. These are the minimum capabilities necessary; some EHRs will have additional security capabilities.

- Access control: permit only authorized users to access electronic health information
- Emergency access: permit authorized users to access electronic health information during an emergency Automatic log-off: end an electronic session after a predetermined time of inactivity

- Audit log:
  - Record actions related to electronic health information
  - Enable a user to generate an audit log for a specific time period and to sort entries
- Integrity: verify that electronic health information has not been altered in transmission and detect the alteration of audit logs
- Authentication: verify that a person seeking access to electronic health information is the one claimed and is authorized to access the information
- Encryption for general information
- Encryption when exchanging electronic health information
- Accounting of disclosures [optional]: record disclosures made for treatment, payment, and health care operations

While a certified EHR provides considerable security capabilities, you will still need to comply with the other administrative and technical safeguards to ensure the privacy and security of your patients with HIV/AIDS. In addition, you and your staff should be trained to comply with these protections. Online tools and resources (see Related Resources below) can be used to develop one-on-one or group training. In addition, the HITECH Act funds technical assistance and training programs to support meaningful use of EHR technologies. Two of these programs offer privacy and security compliance training and will assist you to implement privacy and security protections:

Regional Extension Centers (RECs) – ONC has funded 62 RECS across the country to support the adoption and meaningful use of EHRs. The RECs provide outreach, education, and technical assistance to help providers adopt EHRs and use them in a meaningful way. All RECs are required to educate providers on best practices related to privacy and security. In addition, ONC has worked collaboratively with the RECs to develop tools related to risk identification and mitigation both during and after implementation. The RECs focus their technical assistance on primary care clinicians and will assist clinicians working in safety net and community health center environments. State-by-state REC contact information is included on this website.

Strategic Healthcare IT Advanced Research Projects on Security (SHARPS) – SHARPS is a four-year research project supported by ONC aimed at reducing security and privacy barriers to the meaningful use of health IT. The project is led by the University of Illinois at Urbana-Champaign. The SHARPS website contains a list of publications by members of the team on a range of health IT security topics.

Related Resources:

HIPAA Security Series – This CMS series includes seven educational documents designed to give HIPAA entities insight into the Security Rule and assistance with implementation of the security standards. Topics include: Security 101 for Covered Entities; Administrative Safeguards; Physical Safeguards; Technical Safeguards; Organizational, Policies and Procedures and Documentation Requirements; Basics of Risk Analysis and Risk Management; and Security Standards: Implementation for the Small Provider.
Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices – This ONC guide assists small health care practices to reassess their existing health information security policies for adopting and implementing EHRs. It includes frequently asked questions to help your practice identify appropriate safeguards and conduct risk assessments to secure electronic health information.
Technical Guidance for HIV/AIDS Surveillance Programs: Security and Confidentiality Guidelines – This Centers for Disease Control

and Prevention (CDC) document for State and other governmental staff provides a set of guidelines for HIV/AIDS Surveillance Programs on confidentiality and security while conducting HIV/AIDS surveillance. Included is a Security and Confidentiality Program Requirement Checklist.

Ensuring Security of High-Risk Information in EHRs – This article discusses security precautions when dealing with sensitive protected health information.

HIV/AIDS Confidentiality and Data Security Guidance – This guidance document is targeted to local health departments and community based organizations that are developing, implementing, and maintaining policies and procedures to protect HIV/AIDS client confidentiality and medical records.

Developed by the Health Resources and Services Administration as a resource for health centers and other safety net and ambulatory care providers who are seeking to implement health IT.

EXHIBIT 8

HIPAA & Security

Many health care organizations find themselves scrambling to prepare their information systems to help them meet the next HIPAA regulation deadline. These administrative standards for regulating the storing and transmitting of patient information require organizations to adapt processes throughout the care continuum. MEDITECH's tightly integrated system provides the tools to help staff meet these requirements.

MEDITECH offers HIPAA-compliant versions of EDI transactions, including claims submissions, remittance transactions, and health care eligibility transactions. Our system also enables organizations to honor privacy rights by enabling patients to opt out of hospital directories; using medical record numbers, rather than patient names, in reports; and flagging VIP/confidential patients.

Additionally, the MEDITECH system incorporates multi-tiered access control features that provide protection across all levels and types of access, as well as system-wide audit trails that track the viewing and editing of data.

Related News

CMS To Delay Enforcement of HIPAA 5010 by 3 More Months ***New***

Civil Liberties Union Criticizes N.Y.'s Health Data Exchange Policies ***New***

Study Finds More Work Needed To Boost Patient Control of Health Data ***New***

MEDITECH

Electronic Health Record

Functionality Brief

MEDITECH's Electronic Health Record (EHR) captures and shares real-time patient information across the continuum and makes it available to care providers directly through their respective applications. At the center of our EHR is a longitudinal clinical record, which consolidates patient information from across applications and enables physicians, clinic-based caregivers, home health staff, clinicians, and other authorized providers to simultaneously view current and lifetime information from one central location.

Highlights:

- Access fully integrated clinical, historical, and outpatient data from any location
- View real-time data for visits conducted anywhere across the continuum of care
- Organize meaningful data into standard and customizable clinical panels
- Trend patient data using graphs, flowsheets, and lifetime result views
- Receive automatic clinical alerts for new and abnormal results
- Combine, archive, and report on discrete data throughout the continuum of care
- Protect security of patient information through user-defined access
- Combine data captured across the MEDITECH EHR with other vendor data

The Electronic Health Record Enables Care Providers to:

Access Real-time Patient Records

The clinical record component of our EHR gives your care providers immediate access to real-time critical information to support more informed decision making regarding patient assessments and treatments. Information collected in the patient's record includes, but is not limited to:

- Vital signs and I&O data
- Medications, including a view-only format identical to the Medical Administration Record
- Lab results, including Blood Bank, Pathology, and Microbiology
- Reports and patient notes, including diagnostic imaging with links to PACS images
- Patient care activity (assessments, outcomes, plans of care)
- Patient history and administrative information
- Order history (acute and ambulatory).

Ensure Security of Patient Records

The EHR protects the security and confidentiality of patient information by establishing roles-based access and restrictions. For example:

- User access can be restricted based on patient and/or location
- Confidential patient and VIP flags may be used to prevent users from accessing the records of patients located within confidential locations or who have been assigned a confidential status
- Users may be restricted to viewing only those patients located within a designated nursing unit or assigned to a specified physician.

Perform Quick Patient Summary Reviews

From the EHR's clinical record care providers can access a summary of their patients' current activity, as well a snapshot of their complete visit histories. Care providers can easily drill down into each visit to view more detailed information, such as test results and vitals signs. A centralized Patient Summary list grants care providers instant access to a patient's:

- Current and ongoing problems
- Allergies and adverse reactions
- Medication history
- Pharmacy information and location
- Health maintenance
- Legal, demographic, and referral data
- Growth charts
- Confidential patient notes
- Substance use
- Current and past procedures
- Diagnosis and codes.

Organize Data Using Clinical Panels

Flexible clinical panels are designed to group patient data into clinically meaningful displays where clinicians can compare all facets of patient data, making it easier to trend and interpret information. Clinical Panels provide detailed, user-friendly spreadsheets, which contain a wide range of patient information, such as medication administrations and test results that reflect common evaluations and might normally be viewed on separate panels. For example, a single clinical panel might include Respiratory, Neurological, Intake and Output, and Diagnostic Report information.

In addition, providers can tailor their own customized clinical panels to view specific information based on their unique specialties, such as dietary or respiratory therapy, as well as establish default panels to support their workflow.

Trend Current and Historical Patient Data

Care providers can review complete visit histories across the healthcare continuum. Users can select the visit(s) for which they want to see patient information, or they can request a compilation of data from all visits. This data includes medical history, test results, abstracts, and demographics.

In addition, care providers can select a subset of data and use it to:

- Graph current and historical clinical results over time
- Search for associated on-line clinical content, such as evidence-based medicine
- Streamline documentation by saving and incorporating this data into patient notes and reports.

Clinicians can also select a Lifetime View option for multiple clinical panels, such as Medications, Laboratory, Microbiology, Blood Bank, and Reports, enabling them to display all historical results for a specific test or report. A new results panel is also provided for clinicians to view results from the last 24 to 48 hours, or any information that is new to them.

Exchange Real-time Information between Care Settings

To support interoperability with other vendor systems, MEDITECH also offer a Continuity of Care Document (CCD) exchange suite for querying and pulling in External Medical Summaries (XMS) of past patient visits from other vendor systems. These XMS documents are accessible from both the Clinical Patient Summary and the Reports section of the EHR's clinical record and include such information as:

- Allergies
- Current medications
- Problem lists
- Advanced directives
- Immunizations
- Active conditions
- Visit history
- Discharge summaries.

Reap the Benefits of Integration

The EHR's clinical record provides a central clinical repository for housing real-time patient information captured throughout our system. The clinical record can be accessed, viewed, and edited by all authorized staff from within the ancillary, clinical, and administrative applications. In turn, information updated in the EHR is pushed out to other applications in real time through roles-based desktops and status boards to help your care providers provide timelier and better coordinated care. From within their respective applications, care providers can instantly drill down into a patient's clinical record, making detailed patient information always just a click away. Care providers can also graph and trend clinical information, such as vitals signs, results, and I&O data. Real-time patient information is accessible during the entire documentation process to view a patient's progress. Tight product integration with CPOE, Pharmacy, and Bedside Verification also creates a closed-loop medication management system, effectively circumventing medication errors when reconciling, ordering, filling, and administering medications.

For more information about us, contact a MEDITECH Marketing Consultant.

MediTech Data International

search this site Submit Query

Electronic Medical Records Specialist Group

RSS

- **Medical Records**

  Electronic Medical Records EMR

- **Data Entry**

  Quality Data Entry Services

- **Electronic Files**

  Document Management

- **RFID & Barcodes**

  RFID and Barcode Management

- **Contact Us**

  800-545-0868 Request Info

MDi

- Client Support
- About MDi

Electronic Files

Dealing with documents and information **can be one of the most challenging aspects of business.** The Meditech Data (MD-EDMS) document management solution will improve how you process this information.

Simplify your office by routing paper documents, e-mails, and other files directly into **MD-EDMS.** Eliminate wasted time searching for paper and replacing lost documents.

Access your information the moment you need it, Applications that capture paper and electronic documents and provide the storage, retrieval, security and archiving of those documents. Records management is a specialized discipline.

Electronic Documents Management Systems (EDMS):

Document management systems are software applications that capture paper and electronic documents and provide the storage, retrieval, security and archiving of those documents. Records management is a specialized discipline. In particular, it is a set of recognized practices related to the life cycle of records – information that serves as evidence of the business activities of an organization.

The document management process begins with the conversion of paper documents and records to electronic files. Digitizing eliminates the many obstacles created by paper – labor-intensive duplication procedures, slow distribution, misplaced originals and the inconvenience of retrieving files from remote locations. Because paper files are also costly to process, duplicate, distribute and store, digitizing reduces operating expenses and overhead. Document management applications enable more efficient distribution of and control over information, files and records throughout the organization.

These software programs simplify business processes by automating repetitive procedures, document routing and email notification. Document management systems expedite business processes by allowing instant access to information; greater collaboration within and among departments and offices; enhanced security for files and records; and the application of procedures that facilitate compliance with record-keeping requirements by major companies of the world.

Benefits of Document Imaging

Thousands of organizations around the world use document imaging every day instead of paper filing systems. Document imaging offers a number of benefits over paper or microfilm systems.

Fast Retrieval

Imaging lets you find documents quickly without leaving your desk. Paper and microfiche are slower because users must go to files and search manually.

Flexible Indexing

Imaging can index documents in several different ways simultaneously. Indexing paper and microfilm in more than one way is awkward, costly and time-consuming.

Full-Text Search

Imaging systems can retrieve files by any word or phrase in the document, a capability that is impossible with paper or microfiche.

No Lost Files

Imaged documents remain in their folders when being viewed, so none are lost or misplaced. Plus, index template and full-text searches can find documents if they are accidentally moved. Lost documents are expensive and time-consuming to replace.

Digital Archiving

The risk of loss or damage to paper or electronic records is reduced with a document imaging system. Keeping archival versions of documents in a document imaging system helps protect paper documents from over-handling and keeps electronic documents in a non-proprietary format.

Share Files Easily

Imaging makes it easy to share documents electronically with colleagues and clients over a network, on CD or through the Web. Paper documents usually require photocopying to be shared, and microfilm requires conversion to paper.

Improved Security

Imaging can provide better, more flexible control over sensitive documents. Imaging controls security at the folder, document or individual word level for different groups and individuals. In contrast, all paper
documents in a filing cabinet or filing room have the same level of security.

Save Space

Imaging will help recover valuable office space that was previously taken up by bulky paper files.

Disaster Recovery

Imaging provides an easy way to back-up documents for offsite storage and disaster recovery. Paper is a bulky and expensive way to back-up records and is vulnerable to fire, flood and theft.

- Latest
- Popular
- Upcoming
- MediTech Data International
- Medical Records 0 comment(s)
- Electronic Files 0 comment(s)

Check back for the most up to date information about upcoming events!

- **IT Solutions**

  - IT solutions for Healthcare, finance and legal entities. We design and implement the infrastructure for business such as small and medium scale enterprise solutions.

- **Helpful Resources**
  - coming soon

- **Categories**
  - Updates (1)

Follow MDi

- Facebook
- Twitter
- Linked In

Popular Tags

Document Management Systems Data Entry Electronic Medical Records RFID and Barcode Management

- Client Support
- About MDi
- Contact MDi
- Sitemap

© MediTech Data International - All rights reserved | License # 21005
Special thanks to: Anyth.ingBy.Us
Orginal theme by: The Forge Web Creations

EXHIBIT 9

THE STATE OF NEW HAMPSHIRE

MERRIMACK, SS SUPERIOR COURT

Docket No. 217-2012-CV-00617

EXETER HOSPITAL, INC.

v.

DR. SHARON ALROY-PREIS, ET AL.

AFFIDAVIT OF SHARON ALROY-PREIS, M.D., MPH

I, Sharon Alroy-Preis, upon oath do hereby depose and state as follows:

1. I am the State Epidemiologist for the State of New Hampshire, Department of Health and Human Services, Division of Public Health Services ("Public Health"). I am a licensed physician trained in Internal Medicine, Infectious Disease and Preventive Medicine and, in addition, have earned a Master in Public Health.

2. My responsibilities as State Epidemiologist include medical and epidemiological supervision and administrative oversight of the Communicable Disease Control, Communicable Disease Surveillance, Immunizations, HIV/STD and Food Protection units. Among other things, my duties include directing field activities for disease outbreak investigations, overseeing analysis of those investigations, and instituting appropriate prevention and control measures as well as providing consultation and technical assistance to field staff and other epidemiology staff regarding disease surveillance, prevention, and control measures. Since accepting my appointment for the position of State Epidemiologist, I have overseen more than 250 Public Health investigations. In my capacity, I serve as the New Hampshire contact person for the Centers for Disease Control and Prevention ("CDC") in matters of communicable diseases and in

charge of reporting to the CDC outbreaks and cases of reportable diseases that occurred in New Hampshire.

3. On May 15, 2012, Exeter Hospital reported to Public Health a cluster of four cases of recently diagnosed hepatitis C at Exeter Hospital.

4. Hepatitis C is a viral infection that can cause liver disease. In cases of active infection, the virus can be found in the infected person's blood. Most people who acquire hepatitis C do not have any symptoms at all. The virus infects a person's liver causing inflammation that can result in damage to the liver tissue. While some people will never have complications from chronic hepatitis C infection, in others the infection may result in liver cirrhosis, liver failure, liver cancer or death. Some people with chronic infection can be treated with effective antiviral medications.

5. As a result of Exeter Hospital's report, Public Health began an investigation to determine whether the cluster is truly an outbreak. Once Public Health determined that the initially reported cases were related, the goals of the investigation have been: (1) to stop transmission of the infection by establishing, and disrupting, the mode of transmission, and (2) to determine the scope of the outbreak by identifying all those impacted and those actively infected to allow linkage to appropriate care. It is standard practice in epidemiological investigations to identify and classify those impacted into three categories: confirmed, probable and suspect/possible cases.

6. In its investigation, Public Health has been utilizing various methods to achieve the above mentioned goals including site visits to different patient care units in Exeter Hospital, observations of relevant procedures, interviewing hospital employees and patients, reviewing hospital policies and procedures and reviewing relevant patient medical records.

7. Beginning in May, as part of its routine outbreak investigation process, Public Health established routine communication with Exeter Hospital. Communication included daily conference calls to discuss relevant updates and to inform Exeter Hospital on the course of the investigation. The updates included public health recommendations on testing, the reasoning for those recommendations and appropriate disease control measures. Important information on conducting and furthering the outbreak investigation were also provided to Exeter Hospital during these conference calls including; requests for information to advance the investigation, testing algorithms, communications to healthcare providers regarding the outbreak, hepatitis C education materials developed to inform the public on the outbreak and advance copies of press releases issued by Public Health regarding the investigation.

8. On June 12, 2012, to facilitate communication with Exeter Hospital regarding the investigation while maintaining security and confidentiality, Public Health implemented and hosted a secure file transfer protocol ("FTP") exchange server. Public Health's requests containing confidential information have been uploaded on the exchange server site to be accessed securely and exclusively by Exeter Hospital.

9. Early in the investigation when Public Health requested review of medical records, Exeter Hospital provided access to records stored both electronically and on paper. From May through July, Exeter Hospital did not require disclosure of the specific records or the portions of those records to be reviewed prior to making the records available to Public Health investigators. Rather, Exeter Hospital provided open access upon being informed that the review was in furtherance of the hepatitis C outbreak and investigation.

10. As a result of its early investigation, Public Health determined that the cases reported by Exeter Hospital (3 patients and 1 healthcare worker) were part of an outbreak:

Molecular testing at the Public Health lab revealed that all four individuals had identical sequence of the virus, indicating a common source of infection, and epidemiological investigation revealed they all shared a common link: being in the hospital cardiac catheterization laboratory (CCL) or its recovery room (RR). Based on the epidemiological investigation (which included medical record review), Public Health was able to determine that the most likely mechanism of transmission is narcotic diversion by the HCV positive healthcare worker.

11. In addition to medical record reviews, hospital employee interviews and other investigative methods (described above), Public Health tested (as of August 15th, 2012) 1,144 persons of the 1,293 who were recommended by Public Health for testing because they were either CCL/RR patients (1066) or employees (78). As a result of this testing, Public Health has already identified 33 people with an active HCV strain that matches the outbreak strain and 28 additional patients who have evidence of a past HCV infection that has cleared. Because it is not possible to conduct molecular tests (virus sequencing) for patients with cleared infections, additional epidemiological investigation including medical record review is necessary to determine whether the infection in these patients might have been acquired as part of this outbreak.

12. Based on information from the ongoing investigation, Public Health discovered that the healthcare worker suspected of narcotic diversion may have also been present in the main inpatient operating room (OR) and the intensive care unit (ICU) at Exeter Hospital. Given this new information, Public Health recommended, and is in the process of, testing patients who received care in these areas during the time of employment of the implicated healthcare worker. Outstanding questions remain regarding the mode of transmission and the scope of the outbreak.

This is an ongoing investigation that will require gathering additional information from Exeter Hospital, its employees and regional providers as well as state and federal agencies, including the CDC. The entire scope of the outbreak is yet to be determined to assure no other patients, in other patient care areas, may have been exposed.

13. In early August, Exeter Hospital agreed to provide Public Health investigators involved in medical record reviews individualized user names and passwords for access to EMR. A request for such individualized credentials was first made by Public Health in June. Each Public Health investigator signed an "End User Security Agreement – Outside Individual Access" so that they would be able to access electronically maintained medical records by use of an individualized login name and password. By providing user name and password for the relevant Public Health investigators, Exeter Hospital can audit their access to records.

14. In July and August, Exeter Hospital began asking Public Health to provide information about facts learned in the investigation regarding specific patients including the results of tests performed by Public Health. After Public Health told Exeter Hospital that it was prohibited from sharing such personal health information under RSA 141-C:10, Exeter Hospital began resisting Public Health's requests. Among other things, Exeter Hospital refused to allow further interviews of its staff unless such interviews were monitored by an Exeter Hospital representative and it refused to provide access to patient medical records unless Public Health first provided evidence sufficient for Exeter Hospital to conclude that the information requested was definitely linked to the established outbreak. This included refusal to allow access to medical record of certain patients in order to determine if other patients might have been exposed to the activities of the implicated healthcare worker, putting them at risk for acquiring hepatitis C.

15. On August 24, 2012, Exeter Hospital was notified that Public Health would be making a site visit at Exeter Hospital to review the records of a specific patient. In the notice, Exeter Hospital was notified that the purpose of the review was for "[o]utstanding questions regarding possible exposure to HCV at the hospital" and that "[t]his record review falls within the purview of the HCV outbreak investigation and [Public Health] will review no more than the necessary information." When the Public Health employee arrived at Exeter Hospital, she was met by counsel for Exeter Hospital who told her that unless she provided additional information about her review including specific information as to "why this patient is connected to the DPH investigation" she would not be allowed access.

16. More recently, Exeter Hospital has used the litigation as an excuse to absolutely refuse to provide any information to Public Health regardless of whether Public Health provides details on the reasons and scope of records to be reviewed (as previously outlined by Exeter Hospital's counsel).

Date: 10/2/2012

Sharon Alroy-Preis
New Hampshire State Epidemiologist

THE STATE OF NEW HAMPSHIRE
MERRIMACK, SS.

On the 2nd day of October 2012, before me the undersigned officer, appeared Sharon Alroy-Preis known to me (or satisfactorily proven) to be the person whose name appears above, and she subscribed her name to the foregoing instrument.

Richelle R. Swanson
Notary Public/Justice of the Peace
My Commission Expires:

RICHELLE R. SWANSON, Notary Public
My Commission Expires October 8, 2013

Printed Name: Richelle R. Swanson

EXHIBIT 10

THE STATE OF NEW HAMPSHIRE

MERRIMACK, SS SUPERIOR COURT

Docket No. 217-2012-CV-00617

EXETER HOSPITAL, INC.

v.

DR. SHARON ALROY-PREIS, ET AL.

AFFIDAVIT OF ELIZABETH R. DALY, MPH

I, Elizabeth R. Daly, upon oath do hereby depose and state as follows:

1. I am the Chief of the Infectious Disease Surveillance Section, and the Director of the Epidemiology Branch with the Operations Section of the HCV Investigation Incident Command Structure. In this role, I provide epidemiologic oversight to Epidemiology Branch staff and guide the epidemiologic investigation activities related to the HCV investigation under the direction of the Operations Section Chief, Christine Adamski, and the Incident Commander, Dr. Sharon Alroy-Preis.

2. I have a Master of Public Health degree in epidemiology and have managed and led the investigation of more than 40 infectious disease outbreaks and provided epidemiologic oversight and recommendations for public health response for an additional 300 infectious disease outbreaks investigated by the New Hampshire Department of Health and Human Services ("NH DHHS").

3. With respect to NH DHHS investigation into the hepatitis C outbreak at Exeter Hospital, I directed and participated in medical record review.

4. The first site visit at Exeter Hospital (EH) for medical record review occurred on May 31, 2012 with the goal of understanding the risk factors of the first four cases identified to

inform a strategy of identifying and testing other similarly at-risk patients. Prior to this date, clinical information was obtained on the four initial reported cases from the healthcare institutions where the patients were diagnosed, including EH.

5. Most subsequent EH site visits were arranged on the daily conference calls that occurred between NH DHHS and EH. In addition to this planning call, the medical record review team communicated directly with the EH Infection Preventionist (IP) by phone, email, or in-person while on site visits to plan the next site visit. A written list of patients to be or who had been reviewed was not provided to EH administration before, during, or after any site visit, nor was the reason for the review of each record.

6. The EH IP was assigned to assist the medical record review team on-site. The team worked in the Infection Prevention and Hospitalist Services suite on the second floor. The team consisted of one to six persons (average two to three). The IP identified vacant workstations for the team to sit at for computer access to the Electronic Medical Record (EMR). The IP logged each team member into the EMR using the IP's credentials. The secondary IP logged team members in when the IP was not available. The IP left the team to complete EMR reviews independently, but was available nearby when questions or problems arose. Each medical record review ranged from 10 minutes to 2 hours, depending on the complexity and documentation of the patient's history.

7. On June 12, 2012, NH DHHS asked EH for individual logins for specific DHHS investigators for several reasons, including 1) to avoid having team members get locked out of the computer and be unable to complete work if the IP was not available to log the team member back in, and 2) to create an audit trail of who accessed the patient EMR, as required by HIPAA. This request was denied.

8. This review process as described above was routine except for two exceptions.

1. On Saturday, July 14, 2012, I made an urgent site visit to investigate Case 32. Barbara Hughes brought me to her office in the executive suite where Ms. Hughes logged in to the EMR using her own credentials. Ms. Hughes then observed the EMR review. At the completion of the review for Case 32, which took approximately 1.5-2 hours, the team member told Ms. Hughes that there were 5 additional people to look up in the EMR because these were past CCL employees who were indicated for testing that had not been HCV tested yet because they refused or specimen collection could not be arranged. The employee's medical record was accessed to look for evidence of hepatitis C infection, which was critical to the NH DHHS investigation to explain the source for case 32's infection.

2. On Friday, July 27, 2012, a NH DHHS infectious disease physician was dispatched to EH to conduct medical record review of three patients that were of critical importance to the public health investigation based on new information from CDC on their testing results. On this day, the NH DHHS physician was provided with login credentials and access to the EH EMR.

9. On July 28, 2012 a full list of the medical record review team (8 NH DHHS staff) was provided to EH so that login credentials could be created for each person. EH asked each person to complete an End User Agreement, which was signed and returned on August 15th, 2012. No medical record reviews were made during this time (July 28-August 15) because NH DHHS was waiting for the creation of these individual logins. NH DHHS requested medical record review site visits on several occasions, some of which were agreed to by EH but were later postponed and eventually refused by EH.

10. On August 29, 2012, EH filed a protective order to prevent NH DHHS from reviewing patient medical records. As such, the last medical record review site visit occurred on July 27, 2012.

11. Medical record reviews are conducted for any patient suspected to be related to the EH hepatitis C investigation to fulfill the public health purposes of:

- Defining the extent of the outbreak
- Identifying and recommending testing for exposed persons

- Identifying the source of the outbreak
- Identifying risk factors associated with the outbreak, and
- Protecting the public and controlling the outbreak to prevent additional infections.

12. The types of patients whose medical record review contributes to this purpose include those EH patients who:

- Were reported by EH as being possibly associated with the suspected outbreak
- Were exposed and tested positive for hepatitis C virus
- Were exposed and died
- Were exposed and not tested for hepatitis C virus
- Died with hepatitis
- Were not known to be exposed but were diagnosed with hepatitis C virus at EH's Laboratory
- Were seen in the Emergency Department for hepatitis
- May have been exposed based on epidemiologic information, or
- Are EH employees that could be a source of the outbreak based on epidemiologic information or could have been exposed themselves as part of their medical care at EH.

13. Medical record review team members used EH's EMR (called Meditech) to collect case information including: patient demographics, underlying medical conditions, laboratory testing information, procedure notes, nursing notes, medications (discontinued and current), hepatitis C risk factors, previous hepatitis C diagnoses, and information on the types of exposures (visits, admissions, surgical and diagnostic procedures, etc) that patient had at EH. Additionally, there were other sources of patient information outside of the EMR that NH DHHS did not have electronic access to and made requests for hard copy records. These included the CCL's independent electronic documentation system (called MacLab), Live Patient Activity system, and pharmacy records from the automated medication dispensing system (called PYXIS). There are likely additional sources of data that will need to be accessed for future medical record review based on the patient's exposure (for example, any operating room data systems, endoscopy suite data systems, etc.).

14. There were several tools developed to collect relevant patient information from the EMR. These tools included both paper forms and electronic forms (*i.e.,* databases). These tools were used to prevent the need to print or request hard copies of the patient's entire medical record, which would have been the alternative to conducting electronic medical record review.

Paper Forms. Paper forms were used to collect information on patients that were possibly exposed or possibly infected with hepatitis C and were identified through active surveillance approaches (review of emergency department, laboratory, and death data). The forms used were:

- Death Medical Record Extraction Tool (2 pages): Used to review medical records for exposed patients that died and other EH patients that died from a hepatitis-related cause. The form collects demographics, death information, possible hepatitis C-related symptoms, past history of hepatitis C, hepatitis C test results, liver enzyme function test results, and hepatitis C risk factor information.

- HCV Medical Record Extraction Tool (2 pages): Used to review medical records for patients diagnosed with hepatitis C in the EH laboratory. The form collects demographics, past history of hepatitis C, hepatitis C test results, liver enzyme function test results, hepatitis C risk factor information, and information on EH exposures (ED visits, hospitalizations, medical procedures) since January 1, 2009 and related controlled substance drug administration associated with these exposures.

- Emergency Department Encounter Follow-up Form (1 page): Used to review medical records for patients seen in the EH emergency department for hepatitis-related conditions as identified in the NH DHHS Automated Hospital Emergency Department Data System. The form collects demographics, past history of hepatitis C and associated symptoms, hepatitis C test results, hepatitis C risk factor information, and information on recent healthcare exposures (ED visits, hospitalizations, medical procedures).

Electronic Forms. An electronic database was used to collect information on exposed patients that tested positive for hepatitis C virus. This electronic database was created in a Centers for Disease Control and Prevention software program called EpiInfo with data stored in a Microsoft Access database. These databases were loaded on State of NH issued encrypted and secure laptops and brought to EH. The medical record review team entered data from the EMR directly into the database on these laptops, which were returned to the NH DHHS office for combining of patient information and data analysis. This database contains 549 variables/data points and is 14 "pages" long. In brief, the database collects demographics, past history of hepatitis C, hepatitis C test results, liver enzyme

function test results, hepatitis C risk factor information, underlying medical conditions, medications, and information on EH exposures (ED visits, hospitalizations, medical procedures) since January 1, 2009 and related controlled substance drug administration associated with these exposures.

15. Since the beginning of the hepatitis C investigation, the medical record review team has completed medical record review on 135 patients at EH. The types of EH patients reviewed include:

Type of Patient	**Number Reviewed**
Patients reported by EH as being possibly associated with the suspected outbreak	5
Exposed patients that have tested positive for hepatitis C virus	58
Exposed patients that died	23
Exposed patients not tested	1
Patients that died from a hepatitis-related cause	3
Patients diagnosed with hepatitis C virus at EH's Laboratory	36
Patients seen in the Emergency Department for hepatitis	3
Patients who may have been exposed based on epidemiologic information	0
EH employees that could be a source of the outbreak based on epidemiologic information or could have been exposed themselves as part of their medical care at EH	6

16. Medical record review site visits occurred every week or two depending on need. Medical record reviews occurred on at least ten dates, which were 05/31/2012, 06/13/2012, 06/14/2012, 06/28/2012, 07/03/2012, 07/11/2012, 07/14/2012, 07/16/2012, 07/26/2012, and 07/27/2012.

Date: 09/13/2012

Elizabeth R. Daly, MPH

THE STATE OF NEW HAMPSHIRE
MERRIMACK, SS.

On the 13th day of September 2012, before me the undersigned officer, appeared Elizabeth R. Daly known to me (or satisfactorily proven) to be the person whose name appears above, and she subscribed her name to the foregoing instrument.

Notary Public/Justice of the Peace
My Commission Expires: July 14, 2015
Printed Name: Cheryl J. Storey

CHERYL JEAN STOREY, Notary Public
My Commission Expires July 14, 2015