Transmission of Protected Health Information During Incidents by Amateur Radio

Gordon L. Gibby MD KX4Z

v. 1.0 May 9 2019
v. 1.1 Dec 10, 2020 – spelling errors corrected, additional emphasis added on the requirement for error-free transmission.

DISCLAIMER: The following is my best understanding of the laws and rules that pertain in the United States, but I am not a lawyer and this is not legal advice.

BACKGROUND

The "Privacy Rule" was born out of federal statute requiring safeguards to the privacy of patients as follows:

> *The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information. Collectively these are known as the Administrative Simplification provisions.*
>
> *HIPAA required the Secretary to issue privacy regulations governing individually identifiable health information, if Congress did not enact privacy legislation within three years of the passage of HIPAA. Because Congress did not enact privacy legislation, HHS developed a proposed rule and released it for public comment on November 3, 1999. The Department received over 52,000 public comments. The final regulation, the Privacy Rule, was published December 28, 2000.*[2]
>
> *In March 2002, the Department proposed and released for public comment modifications to the Privacy Rule. The Department received over 11,000 comments. The final modifications were published in final form on August 14, 2002.*[3] *A text combining the final regulation and the modifications can be found at 45 CFR Part 160 and Part 164, Subparts A and E.*[1]

APPLICABILITY OF PRIVACY RULE

It has occasionally been argued that the Privacy rule does not apply to amateur radio operators in emergencies.[2] HIPAA Privacy Rule applies to healthcare institutions, business associates, and apparently also to volunteers as follows:

> *HIPAA Applies Only to Covered Entities and Business Associates*
> *The HIPAA Privacy Rule applies to disclosures made by employees, volunteers, and other members of a covered entity's or business associate's workforce. Covered entities are health plans, health care clearinghouses, and those health care providers that conduct one or more*

covered health care transactions electronically, such as transmitting health care claims to a health plan. Business associates generally are persons or entities (other than members of the workforce of a covered entity) that perform functions or activities on behalf of, or provide certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting protected health information. Business associates also include subcontractors that create, receive, maintain, or transmit protected health information on behalf of another business associate. The Privacy Rule does not apply to disclosures made by entities or other persons who are not covered 4 entities or business associates (although such persons or entities are free to follow the standards on a voluntary basis if desired). There may be other state or federal rules that apply. [3]

Not being a lawyer, I am unable to review whether this applies to amateur radio volunteers who either are, or are not, recognized volunteers for a particular hospital. It would appear to more apply to volunteers who ARE trained and credentialed by a particular hospital, and perhaps less so to volunteers for a completely different organization call in, during an incident, to help with treatment of patients threatened by some event. However, without knowing applicable case law decisions, I can't be certain of these ideas.

Note that the Privacy Rule concerns when you can DISCLOSE information that is personally identifiable protected health information. Disclosing includes sending that information to a physician or others at a different health care institution for the purpose of TREATMENT of the patient. This is a clearly allowed transfer of information which no person in their right mind would oppose. [4] The patient's life or safety may well depend on the other physician sending or receiving complete information.

Definition of Treatment:

> ***Treatment*** *is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.* [5]

As should be obvious, TREATMENT is a specifically allowed reason to disclose protected healthcare information. Almost all Americans have seen this, when their referring physician sends records to a specialist called in for a specific health care issue.

> ***Treatment, Payment, Health Care Operations.*** *A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.*[19] *A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship. See additional guidance on Treatment, Payment, & Health Care Operations.* [6]

Note: it is important to note, that even the Privacy Rule (which controls disclosures) doesn't penalize every single incidence of accidental disclosure – but sending records from one institution to another, by amateur radio, during an incident is an INTENTIONAL and PERMITTED disclosure for TREATMENT

> ***(4) Incidental Use and Disclosure.*** *The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.*[7]

Let me emphasize that again: when protected health information is sent from one institution or one physician to another institution or physician at the direction of those persons, it is a specifically PERMITTED DISCLOSURE for the obvious purpose of TREATMENT of the patient.

SECURITY RULE

It is the SECURITY RULE that defines the protections required when storing or transmitting protected health information.

> *The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.*[8]

There are administrative, physical and technical safeguards required to protect the security of protected health information. Things like lists of who is allowed, locked doors – the one that applies most directly to amateur radio communications during an incident where they have been activated to deal with loss of normal communications, are the technical safeguards contained in 45 CFR Part 164. A key point to learn from 164.306 is that some of these are REQUIRED and some are ADDRESSABLE.

> ***§ 164.306 Security standards: General rules.***
>
> ***(a) General requirements.*** *Covered entities and business associates must do the following:*
>
> ***(1)*** *Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.*
>
> ***(2)*** *Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.*
>
> ***(3)*** *Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.*
>
> ***(4)*** *Ensure compliance with this subpart by its workforce.*
>
> ***(b) Flexibility of approach.***
>
> ***(1)*** *Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.*

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

(c)Standards. *A covered entity or business associate must comply with the applicable standards as provided in this section and in §§ 164.308, 164.310, 164.312, 164.314 and 164.316 with respect to all electronic protected health information.*

(d)Implementation specifications. *In this subpart:*

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification.[9]

Part 164.312 declares the technical safeguards:

§ 164.312 Technical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

(a)

(1)*Standard: Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2)*Implementation specifications:*

(i)*Unique user identification (Required).* Assign a unique name and/or number for identifying and tracking user identity.

(ii)*Emergency access procedure (Required).* Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii)*Automatic logoff (Addressable).* Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv)*Encryption and decryption (Addressable).* Implement a mechanism to encrypt and decrypt electronic protected health information.

(b)*Standard: Audit controls.* Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c)

(1)*Standard: Integrity.* Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2)*Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).* Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d)*Standard: Person or entity authentication.* Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e)

(1)*Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to electronic protected

health information that is being transmitted over an electronic communications network.

(2)*Implementation specifications:*

(i)*Integrity controls (Addressable).* Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii)*Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate [emphasis added][10]

Summarizing the regulation as this applies to amateur radio communications:

Section	Law	Comment
(added Dec 10 2020) 164.306(a) para (1) and (2)	***§ 164.306 Security standards: General rules.*** ***(a)General requirements.*** *Covered entities and business associates must do the following:* ***(1)*** *Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.* ***(2)*** *Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.*	The very first part of protected health information is that it must be handled with systems that insure the INTEGRITY of the information. This is often skipped over by persons with some ulterior motive in attacking this or that radio system or modulation technique. Using systems that do NOT guarantee the correctness of transmission is fraught with risk…. Error correcting systems (not just forward error correction, which is NOT in itself a guarantee) would appear to be required by this regulation….
164.312(a)2(iv)	**(iv)*Encryption and decryption (Addressable).* Implement a mechanism to encrypt and decrypt electronic protected health information.**	Encryption within healthcare facilities is now widely done on laptops etc. However, it is an ADDRESSABLE standard. It is not REQUIRED.
164.312(e)1	**(1)*Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.**	There must be technical security measures to guard against the wrong person gaining access to protected health information being transmitted across electronic systems. Encryption simply isn't even mentioned. Facsimile machines, widely used all across America, are completely unencrypted. If encryption were required, every one of those forwardings of medical information would be prohibited. Physicians talk to one another over non-secure unencrypted telephones, cell phones etc. – if encryption were required, all those conversations would be prohibited.
164.312(e)2(ii)	**(ii)*Encryption (Addressable).* Implement a mechanism to encrypt**	Encryption is specifically listed as ADDRESSABLE – not required! Organizations are instructed to encrypt

	electronic protected health information whenever deemed appropriate	"whenever deemed appropriate". When encryption simply is not reasonable or possible, the organization addresses the issue with an explanation.

Side Note: ARQ (acknowledge / request) transmissions fulfill the spirit of 164.312(e)2(i) which requires methods to avoid corruption of the healthcare information.

So now it is obvious why there is not an "amateur radio exception" to some requirement for encryption – it is impossible to have an "exception" to a non-existent requirement!

Some practices that would be encouraged by the language of 164.312:

No.	Suggestion
1	Transmit protected health information by insecure amateur radio only when necessary for the patient's treatment, after weighing other alternatives – a process that should be completed by the healthcare professionals in consultation with their communications personnel and amateur radio volunteers. (That consultation may be simple: "Nothing else works, doc!"
2	Avoid making the transmission plainly obvious to interlopers – use techniques that are less available to average listener – so avoid AM or SSB or FM voice if possible.
3	If possible, use unusual (but legal) frequencies; for example, short range VHF or UHF might be better than long range HF
4	Use digital techniques, particularly those with ARQ technology to insure the accuracy of the information transmitted for the care of patients.
5.	If directional antennas are a possibility and available, take advantage of them.
6	Do not use excessive power above that required for the necessary and accurate transmission.
7	Use digital techniques that are less-widely available to others where possible – an example would be WINLINK PACTOR, followed by ARDOP or WINMOR

8	Where possible, use peer-to-peer transmissions to a known callsign so that the protected healthcare information is stored on far fewer systems.
9	When the information has been transferred to the appropriate persons, remove it from computers used for transmission to the extent practicable.
10	For pre-planned amateur radio incident support computers, consider encrypting the entire computer and limiting access
11	If information is transferred by a voice relay system, ask intermediate operators to destroy physical copies by shredding or burning.
12	If information is transferred through some central message server, ask the Administrators to avoid displaying the information publicly, and to protect or destroy the stored copies.
13	If information is transferred through a radio-only WINLINK system, ask intermediate operators (if practicable) to remove copies
14	Apply any other practicable steps to protect the confidentiality of protected healthcare information.

Note: Projects/HIPPAHamRadio/EncryptionAmateurRadio.odt

1 U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule. Accessed at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

2 See, for example: http://www.hdscs.org/hipaa.html

3 U.S. Department of Health and Human Services, Office for Civil Rights BULLETIN: HIPAA Privacy in Emergency Situations, November 2014 accessed at: https://www.hhs.gov/sites/default/files/emergencysituations.pdf

4 See, for example this bulletin from the Department of Health and Human Services urging necessary information for the care of patients to be shared, in the wake of Hurricane Katrina: https://www.hhs.gov/sites/default/files/katrinanhipaa.pdf

5 U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule. Accessed at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

6 U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule. Accessed at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

7 U.S. Department of Health and Human Services, Summary of the HIPAA Privacy Rule. Accessed at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

8 U.S. Department of Health and Human Services, The Security Rule. Accessed at: https://www.hhs.gov/hipaa/for-professionals/security/index.html

9 45 CFR Part 164.306 Accessed at: https://www.law.cornell.edu/cfr/text/45/164.306

10 45 CFR Part 164.312 Accessed at: https://www.law.cornell.edu/cfr/text/45/164.312