

DISCLOSURE AND PROTECTION OF HEALTH CARE INFORMATION

What is the Health Insurance Portability and Accountability Act?

The Health Insurance Portability and Accountability Act (HIPAA) is a detailed federal statute, with related regulations, governing access to, disclosure of, and security of a patient's health care information. HIPAA contains both a Privacy Rule and a Security Rule with which physicians must comply.¹

Although the full scope and content of the HIPAA Privacy Rule and Security Rule are beyond the scope of this Guide, physicians and physician groups are well-advised to apprise themselves of the scope and content of the Rules and related regulations and to incorporate their requirements into their practices. The HIPAA Rules and related regulations, among other things:

- Apply to all health information whether electronic, paper or oral.²
- Require physicians to designate a privacy officer to assist staff and patients with questions or complaints as well as to ensure compliance with the HIPAA regulations.³
- Require physicians to designate a security official who is responsible for the development and implementation of the policies and procedures required to comply with the Security Rule.⁴
- Require physicians to ensure the confidentiality, integrity, and availability of all electronic protected health information that the physician creates, receives, maintains, or transmits.⁵
- Require covered entities to create a Notice of Privacy Practices – a HIPAA mandated notice that informs patients about protected health information and their rights, and explains some of the limits on an entity's ability to use and disclose this information.⁶
- Require covered entities to inform patients about the right to request that their PHI not be disclosed to a health carrier, so long as the patient has paid for the services out of pocket. Covered entities and business associates are required to abide by these requests when properly made.⁷

¹ See generally: <http://www.hhs.gov/ocr/privacy/index.html>.

² 45 C.F.R. § 160.103.

³ 45 C.F.R. § 164.530(a).

⁴ 45 C.F.R. § 164.308(a).

⁵ 45 C.F.R. § 164.306(a).

⁶ 45 C.F.R. § 164.520.

⁷ HITECH Act §§ 13405(a); codified at 42 U.S.C. §17935(a).

What constitutes health information, and protected health information, under HIPAA?

“Health information” is defined to include: any information, whether oral or recorded in any form or medium, that is created or received by a health care provider and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of healthcare to an individual.⁸

“Protected health information” is health information, as defined above, that identifies the individual or as to which there is a reasonable basis to believe it could be used to identify the individual, that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium (with limited exceptions).⁹

What is the HITECH Act?

HITECH stands for “Health Information Technology for Economic and Clinical Health,” and it is a new law that was designed to both promote the use of electronic records as a tool for care providers, as well as protect patients’ health information. The HITECH Act establishes payments under Medicare and Medicaid to incentivize using technology properly, strengthens enforcement procedures and penalties, and clarifies disclosure requirements.

What is the GINA?

GINA stands for the Genetic Information Nondiscrimination Act. It was designed to prohibit the use of genetic information for certain health insurance and employment uses. GINA prohibits group health plans and health insurers and even employers from excluding individuals because of their genetic information or disposition to developing a disease in the future.

What is the Uniform Health Care Information Act?

The Uniform Health Care Information Act (UHCIA) is a detailed Washington statute governing access to and disclosure of a patient’s health care information. In 2005, the UHCIA was amended to make the requirements under Washington law more closely aligned with the requirements of HIPAA.

What are recent changes to the laws that regulate health information?

In early 2013, the Department of Health and Human Services (HHS) published a final rule, changing parts of the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules. Some of these are changes required by the HITECH Act or by GINA. These two laws, and the changes adopted by the final rule, reflect the health industry’s growing reliance on electronically stored information, as well as Congress’s concern for patient information to be kept safe.

⁸ 45 C.F.R. § 160.103.

⁹ 45 C.F.R. § 160.103.

Notably, HITECH changes HIPAA's data breach notification requirements, requirements for business associates, restrictions on marketing, revision of the minimum necessary standard, restrictions on the sale of protected health information and Electronic Health Records, requirements for certain requests to restrict use or disclosure of protected health information, provision related to Electronic Health Records, and enhanced enforcement of HIPAA Privacy and Security provisions.

What constitutes health care information under the UHCIA?

Under the UHCIA, "health care information" is defined to include any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient, including a patient's DNA and sequence of chemical base pairs, and directly relates to the patient's health care. The term includes any required accounting of disclosures of health care information.¹⁰

What kinds of requirements do these health care related laws set forth?

HIPAA, UHCIA, HITECH, and GINA set forth specific rules for such things as:

- When a health care provider may disclose a patient's health care information without the patient's consent.¹¹
- What an authorization must contain in order to be valid and permit disclosure of a patient's health care information.¹²
- What a health care provider must do when a patient asks to examine or copy his or her medical record.¹³
- What a health care provider must do when a patient asks to have his or her medical record amended or corrected.¹⁴
- When a health care provider may disclose health care information about a patient to an attorney.¹⁵
- What notice a health care provider must give to patients regarding disclosure of health care information.¹⁶

¹⁰ RCW 70.02.010(7).

¹¹ 45 C.F.R. § 164.512; RCW 70.02.050.

¹² 45 C.F.R. § 164.508(c); RCW 70.02.030(3); RCW 70.02.080.

¹³ 45 C.F.R. § 164.524; RCW 70.02.030.

¹⁴ 45 C.F.R. § 164.526; RCW 70.02.100; RCW 70.02.110.

¹⁵ 45 C.F.R. § 164.512(e); RCW 70.02.060.

¹⁶ 45 C.F.R. § 164.404 (data breach); 45 C.F.R. § 164.528 (accounting); RCW 70.02.020(2) (accounting).

- What a health care provider may charge for duplicating or searching a patient's medical record.¹⁷

What civil and criminal penalties an entity may face when it misuses or inappropriately discloses PHI.¹⁸

Which takes precedence – HIPAA or the UHCIA?

Where HIPAA and the UHCIA provide different privileges, rights or obligations, the law that affords patients the greater access to their own health care information, the greater rights and remedies, or the greater protection of the privacy and security of their health care information governs.

When is it appropriate for a physician to disclose a patient's health care information?

As a general rule under the UHCIA and HIPAA, a physician, an individual assisting a physician in the delivery of health care, or an agent and employee of a physician, may not disclose health care information about a patient to any other person without the patient's written authorization. See a discussion of exceptions to this general prohibition below. Disclosures made pursuant to a patient's written authorization must conform to the terms of the authorization.

What is required for a valid patient authorization under the UHCIA?

To be valid, a patient authorization must generally:¹⁹

- Be in writing.
- Be signed and dated by the patient.
- Identify the nature of information to be disclosed.
- Identify the name, and institutional affiliation of the person, or class of persons, to whom the information is to be disclosed.
- Identify the provider, or class of providers, who is to make the disclosure.
- Identify the patient.
- Contain an expiration date or an expiration event related to the patient or the purpose of the disclosure.

¹⁷ 45 C.F.R. § 164.524(c)(4); RCW 70.02.030(2).

¹⁸ 42 U.S.C. § 1320d-5; 42 U.S.C. § 1320D-6.

¹⁹ RCW 70.02.030(3).

NOTE: The HIPAA Privacy Rules also require a description of each purpose of the requested use or disclosure. The statement “at the request of the individual” is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.²⁰ In addition, the Privacy Rules require that the authorization be written in plain language,²¹ and that a copy of the authorization be given to the patient if the physician seeks an authorization for use or disclosure.²²

What other statements do the HIPAA Privacy Rules require a valid authorization to include?

The HIPAA Privacy Rules require that an authorization must contain statements to place the patient (or representative) on notice of:²³

- The individual’s right to revoke the authorization in writing, and either (i) the exceptions to the right to revoke and a description of how the individual may revoke the authorization; or (ii) a reference to the privacy notice (see below) posted in the physician’s office if the notice includes the rights related to revocation of an authorization.
- The ability or inability to condition treatment, payment, enrollment, or eligibility for benefits on the authorization; and
- The potential for information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient, which would no longer be protected under the HIPAA Privacy Rules.

Must the physician retain a copy of an authorization for release of health care information?

Yes. A health care provider or health care facility must retain the original or a copy of each authorization (or revocation) pertaining to release of health care information.²⁴

How long is a patient authorization to release information valid?

A patient authorization to release information is valid until the expiration date or the expiration event noted in the authorization.²⁵ However, when the authorization permits disclosure to a financial institution or an employer of the patient for purposes other than payment, the authorization as it pertains to those disclosures shall expire 90 days after the authorization is signed, unless renewed by the patient.²⁶

²⁰ 45 C.F.R. § 164.508(c)(1)(iv).

²¹ 45 C.F.R. § 164.508(c)(3).

²² 45 C.F.R. § 164.508(c)(4).

²³ 45 C.F.R. § 164.508(c)(2).

²⁴ RCW 70.02.030(7).

²⁵ 45 C.F.R. § 164.508(c)(1)(v).

²⁶ RCW 70.02.030(6).

When may a patient revoke an authorization to disclose health care information?

A patient may revoke in writing an authorization to release health care information at any time, unless the physician has already taken action in reliance on the authorization or disclosure of information is required for matters related to payments for care that has already been provided to the patient.²⁷ An authorization is no longer valid if it is revoked in writing by the patient before the physician has taken substantial action in reliance on the authorization.²⁸

May a physician be held liable for disclosing information pursuant to a revoked authorization?

Yes, if the health care provider had actual notice that the authorization had been revoked. A patient may not maintain an action against a health care provider, however, for disclosures made in good faith reliance on an authorization if the health care provider had no actual notice that the authorization had been revoked.

What is a breach?

A breach can refer to any acquisition, access, use, or disclosure of patient information (be it the patient's name, address, SSN, or other identifying information²⁹ or health information³⁰) in a manner not permitted by HIPAA. There is a presumption that any impermissible use or disclosure of such information constitutes a breach, which then requires the covered entity to notify the proper parties.³¹

The covered entity may overcome this presumption by demonstrating that there is "a low probability" of risk that the information has been compromised.³² Patients must be notified of a breach, therefore, in every situation when PHI is acquired, accessed, used, or disclosed in a manner not permitted under the Privacy Rule, *except* when a covered entity (or Business Associate, when applicable) demonstrates that there is a low probability that the PHI has been compromised, using an objective risk assessment, based upon at least the following four factors, unless regulatory exclusions apply (see exclusions discussed in the next paragraph):³³

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification,
- The unauthorized person who used the PHI or to whom the disclosure was made,
- Whether the PHI was actually acquired or viewed, and

²⁷ 45 C.F.R. § 164.508(b)(5); RCW 70.02.040.

²⁸ RCW 70.02.040.

²⁹ 45 C.F.R. § 164.514(b)(2).

³⁰ 45 C.F.R. § 160.103).

³¹ 45 C.F.R. § 164.402(1).

³² 45 C.F.R. § 164.402(2).

³³ See definition of breach at 45 C.F.R. §§ 164.402(2)(i)-(iv).

- The extent to which the risk to the PHI has been mitigated.

The covered entity should document and retain the risk assessment in which they engage, and should note additional factors they considered when assessing the risk.

What are the exclusions; what *isn't* considered a breach?

There are three exceptions to the general breach rule:

1. The unintentional use of the information by member of the covered entity's workforce;³⁴
2. Inadvertent disclosure by the covered entity to authorized person;³⁵ and
3. When the recipient does not retain the protected health information.³⁶

It should be noted that the final rule has removed a prior exception that existed for the disclosure of data, so long as the disclosed information did not include any dates of birth or zip codes. Now, a covered entity should always perform a risk assessment after any improper use or disclosure of PHI to determine whether a breach notification should be given.

What kind of notification is a covered entity required to give and when?

When a covered entity discovers a breach, it is required to notify the affected individuals, HHS, and – if appropriate – the media.³⁷ A covered entity needs to keep a record of discovered breaches affecting less than 500 patients, which is submitted to and published by HHS.³⁸

The covered entity is ultimately responsible for notifications, regardless of any business associate involvement or fault. Business associates are responsible only for informing the covered entity of any discovered breach. Media outlets are not required to print or broadcast these notifications, and covered entities are not required to pay for notifications to be printed or broadcasted. Covered entities are, however, required to deliver notice directly to the prominent media outlets being notified.³⁹ Finally, in the event that a notice to a patient is returned to the covered entity as undeliverable, either direct written notice using updated contact information or substitute notice (consistent with regulatory guidelines) must be given within the original 60-day deadline.⁴⁰

Does a patient have a right to be informed of other disclosures of health care information?

³⁴ See definition of breach at 45 C.F.R. 164.402(1)(i).

³⁵ See definition of breach at 45 C.F.R. 164.402(1)(ii).

³⁶ See definition of breach at 45 C.F.R. 164.402(1)(iii).

³⁷ HHS has set forth specific content requirements (45 C.F.R. § 164.404(c)) and methods of notifying individuals (45 C.F.R. § 164.404(d)).

³⁸ HITECH Act § 13402(e)(4); codified at 42 C.F.R. § 17932(e)(3)-(4).

³⁹ 74 FR 42752 (Aug. 24, 2009); 42 U.S.C. § 17932 (e)(2).

⁴⁰ 74 FR 42750-45752. 45 C.F.R. § 164.404(b)

Yes. A patient has a right to receive an accounting of disclosures of health care information made by a health care provider or a health care facility in the six years before the date on which the accounting is requested, except for disclosures:⁴¹

- To carry out treatment, payment, and health care operations.
- To the patient, of his or her own health care information.
- Incident to a use or disclosure that is otherwise permitted.
- Pursuant to a valid authorization where the patient authorized the disclosure of health care information about himself or herself.
- Of directory information.
- To persons involved in the patient's care.
- To authorized federal officials for certain national security or intelligence purposes.
- To correctional institutions or law enforcement officials having lawful custody of the person if necessary for certain purposes.
- Of a limited data set that excludes direct identifiers of the patient or of relatives, employers, or household members of the patient when done so for certain limited purposes.

How must a physician respond to a patient's request for an accounting?

Within 60 days after receipt of a request for an accounting, a physician must provide the accounting requested. If unable to do so within 60 days, the physician may extend the time by no more than 30 days provided that, within the initial 60 days, the physician provides the patient with a written statement of the reasons for the delay and the date by which the accounting will be provided.⁴² Only one such request for an extension is allowed under HIPAA.⁴³

What must be included in an accounting?

The accounting must be in writing and must include:⁴⁴

- The date of disclosure.

⁴¹ 45 C.F.R. § 164.528; RCW 70.02.020(2).

⁴² 45 C.F.R. § 164.528(c)(1).

⁴³ 45 C.F.R. § 164.528(c)(1)(ii)(B).

⁴⁴ 45 C.F.R. § 164.528(b)(2).

- The name of the entity or person who received the protected health information and, if known, the address.
- A brief description of the protected health information disclosed.
- A brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure or a copy of the written request.

May a physician charge for providing an accounting?

The first request for an accounting in any 12-month period must be provided without charge.⁴⁵ Any additional request in the same 12-month period may be subject to a reasonable, cost-based fee provided that the physician informs the patient in advance of the fee and provides the patient the opportunity to withdraw or modify the request in order to avoid or reduce the fee.⁴⁶

Is a specific authorization required for release of some types of health care information?

Yes. Laws other than the UHCIA and HIPAA require specific authorizations for the release of:

- Records of mental health services.⁴⁷
- Records of drug or alcohol abuse treatment and rehabilitation.⁴⁸
- Information regarding AIDS and other sexually transmitted diseases.⁴⁹ See AIDS/HIV/STD.
- A separate authorization is required for the release of psychotherapy notes.⁵⁰

When the patient is a minor, who must provide authorization for release of the minor's health care information?

If the patient is a minor and is authorized to consent to health care without parental consent under federal or state law, only the minor may authorize the release of information pertaining to health care to which the minor lawfully consented.⁵¹ In cases where parental consent is required for the minor's treatment, parental authorization is required for the release of

⁴⁵ 45 C.F.R. § 164.528(c)(2).

⁴⁶ *Id.*

⁴⁷ RCW 71.05.390; RCW 71.05.420; RCW 71.05.630; RCW 71.34.340 (minors).

⁴⁸ RCW 70.96A.150; RCW 70.96A.230.

⁴⁹ RCW 70.24.105.

⁵⁰ 45 C.F.R. § 164.508(a)(2).

⁵¹ 45 C.F.R. § 164.502(g)(3); RCW 70.02.130(1).

the minor's health care information.⁵² See **MINORS, TREATMENT OF** for circumstances in which a minor is authorized to consent to health care.

May a parent obtain access to a child's health care information?

In some circumstances, yes. A minor's parent may obtain access to information pertaining to health care of the minor for which parental consent was required.⁵³ A parent may not, without the minor's consent, obtain access to information about health care of the minor which the minor could obtain without parental consent under state or federal law.⁵⁴ See **MINORS, TREATMENT OF**.

When the parents of a child are legally separated or divorced, which parent is entitled to access to the child's health care information?

Absent a court order to the contrary, each parent is entitled to have full and equal access to the health care records of the child which pertain to health care for which parental consent was required and neither parent may veto the access requested by the other parent.⁵⁵

Who may authorize release of health care information concerning a deceased patient?

The personal representative of the deceased patient or, if there is no personal representative, a person who would have been authorized to make health care decisions for the deceased patient when the patient was alive may authorize the release of health care information about the deceased patient.⁵⁶ Recent amendments to the Privacy Rule now limit the period for which covered entities must protect health information to 50 years after the patient's death.⁵⁷ Additionally, now individuals who were involved in a patient's care or payment for care – but who were not the decedent's personal representative – may request the decedent's records after death.⁵⁸ These kinds of disclosures are permitted, but not required, and need to be relevant to the requesting individual's involvement.⁵⁹ If a physician questions the relationship between the decedent and the requesting individual, the physician may refuse to disclose the information so long as the physician abides by certain requirements.⁶⁰

⁵² *Id.*

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ RCW 26.09.225.

⁵⁶ 45 C.F.R. § 164.502(g)(4).

⁵⁷ 78 FR 5613-5614 (Jan. 25, 2013); 45 C.F.R. 164.502(f).

⁵⁸ 78 FR 5614-5616 (Jan. 25, 2013); 45 C.F.R. § 164.510(b)(5).

⁵⁹ *Id.*

⁶⁰ 45 C.F.R. § 164.524(d).

May a physician disclose health care information to another health care provider without the patient's authorization?

In certain circumstances, yes. A physician may disclose health care information to another health care provider without the patient's authorization to the extent the health care provider needs to know the information in the following circumstances:⁶¹

- If the health care provider is assisting the physician in the delivery of health care and the physician reasonably believes that the health care provider will not use or disclose the health care information for another purpose and will take appropriate steps to protect the information.
- If the physician reasonably believes that the health care provider is providing health care to the patient.
- To the extent necessary to provide health care to the patient if the physician reasonably believes that the health care provider previously provided health care to the patient and if the patient has not instructed the physician in writing not to make such a disclosure.
- If the health care provider is the successor in interest to the physician.

May a physician disclose health care information to a patient's family members without the patient's authorization?

In certain circumstances, yes. If the patient is present or otherwise available prior to such disclosure, the physician may disclose health information if he or she obtains the patient's oral agreement, provides the patient with an opportunity to object and the patient does not object, or the physician reasonably infers from the circumstances, based on professional judgment, that the patient does not object.⁶² If the patient is not present or otherwise available a physician may disclose health care information without the patient's authorization to immediate family members of the patient or to any other individual with whom the patient is known to have a close personal relationship if in the exercise of professional judgment the physician determines that disclosure is in the patient's best interest and the disclosure is limited to that information directly relevant to the person's involvement with the patient's health care, unless the patient has instructed the physician in writing not to make such disclosure.⁶³

Are there other circumstances where a physician may disclose a patient's health care information without the patient's consent?

Yes. Both the UHCIA and HIPAA delineate various other circumstances under which disclosure of health care information may be made without patient consent or authorization.⁶⁴ The circumstances under which such disclosures may be made are fact-specific, sometimes

⁶¹ 45 C.F.R. § 164.506(c); RCW 70.02.050(1).

⁶² 45 C.F.R. § 164.510(b)(2);

⁶³ 45 C.F.R. § 164.510(b)(3); RCW 70.02.050(1)(c).

⁶⁴ 45 C.F.R. § 164.512; RCW 70.02.050

complicated, and not necessarily the same under both statutes. What may be permissible under the UHCIA is not always permissible under HIPAA and vice versa. With that caveat, the following is a general listing of the other types of disclosures that may be permissible under the UHCIA or HIPAA without patient consent under the right circumstances.

Under the UHCIA, a physician may disclose health care information about a patient without the patient's consent to the following persons to the extent they need to know the information:

- To any person who requires health care information for health care education.⁶⁵
- To any person who requires the health care information to provide planning, quality assurance, peer review, or administrative, legal, financial or actuarial services to the physician.⁶⁶
- To any person when the physician reasonably believes the disclosure will avoid or minimize an imminent danger to the health or safety of the patient or any other individual, but there is no obligation to do so.⁶⁷
- To a person for use in a research project that an institutional review board has determined is of sufficient importance to outweigh the intrusion into the privacy of the patient and cannot be done as a practical matter without the use or disclosure of health care information in individually identifiable form, provided certain safeguards against redisclosure are in place.⁶⁸
- To a person who obtains information for purposes of an audit, if the person agrees in writing to remove or destroy, at the earliest practical opportunity, information that would enable the patient to be identified and not to disclose the information further, except to accomplish the audit or to report unlawful or improper conduct involving fraud in payment for health care by the physician or the patient, or other unlawful conduct by the physician.⁶⁹
- To an official of a penal or other custodial institution in which the patient is detained.⁷⁰
- To federal, state, or local law enforcement authorities if the health care provider believes in good faith that the health care information disclosed constitutes evidence of criminal conduct that occurred on the premises of the health care provider.⁷¹

⁶⁵ RCW 70.02.050(1)(b).

⁶⁶ *Id.*

⁶⁷ RCW 70.02.050(1)(d).

⁶⁸ RCW 70.02.050(1)(g).

⁶⁹ RCW 70.02.050(1)(h).

⁷⁰ RCW 70.02.050(1)(i).

⁷¹ RCW 70.02.050(1)(l).

- To another health care provider, health care facility or third-party payor that has a relationship with the patient whose health care information is being requested, if the disclosure is for the purpose of conducting quality assessment and improvement activities, reviewing the competence or qualifications of health care professionals, evaluating practitioner, provider, and third-party payor performance, or conducting training programs.⁷²
- For payment.⁷³

Under the UHCIA, a health care provider or hospital may also report to fire, police, sheriff, or another public authority, that brought a patient to a health care facility or health care provider the patient's name, residence, sex, age, occupation, condition, diagnosis, or extent and location of injuries, whether a patient was conscious when admitted, and the actual or estimated date of discharge.⁷⁴

Under HIPAA, a physician may disclose health care information about a patient without the patient's authorization under certain circumstances:⁷⁵

- When required by law.
- For public health activities.
- When a victim of abuse, neglect or domestic violence.
- For health oversight activities.
- For judicial and administrative proceedings.
- For law enforcement proceedings.
- About decedents.
- For cadaveric organ, eye or tissue donation procedures.
- For research purposes.
- To avert a serious threat to health or safety.
- For specialized government functions.
- For worker's compensation.

⁷² RCW 70.02.050(m); RCW 70.02.010(8)(a)-(b).

⁷³ RCW 70.02.050(1)(n).

⁷⁴ RCW 70.02.050(1)(k).

⁷⁵ 45 C.F.R. § 164.512.

Because the determination of whether the UHCIA and HIPAA permit disclosure of a patient's health care information under any of these circumstances is a fact-specific inquiry that can be quite complicated, physicians are well-advised to consult with legal counsel or someone else well-versed in the UHCIA and the HIPAA regulations before disclosing information in such circumstances without patient authorization.

Under what circumstances must a physician disclose health care information about a patient without the patient's consent?

A physician must disclose health care information about a patient without the patient's consent if the disclosure is:

- To federal, state, or local public health authorities, when the physician is required by law to make the report, or when the disclosure is needed either to determine compliance with state or federal licensure laws or to protect the public health.⁷⁶
- To federal, state, or local law enforcement authorities when the health care provider is required to make the disclosure by law.⁷⁷ See **REPORTING REQUIREMENTS**.
- To federal, state, or local law enforcement authorities, when a patient receives treatment for an injury from a firearm, knife or other sharp object, or a blunt force injury that the authorities reasonably believe resulted from a criminal act.⁷⁸ The authorities must first make a request for such disclosure to a nursing supervisor, administrator, or designated privacy official.⁷⁹ The information to be disclosed, if known, includes the patient's name, address, sex, age, condition, diagnosis or extent and location of injuries, whether the patient was conscious upon admission, the name of the health care provider treating the patient, whether the patient has been transferred to another facility, and the patient's discharge time and date.⁸⁰
- To county coroners and medical examiners for investigation of death.⁸¹
- Pursuant to compulsory process, such as a properly issued subpoena or a court order.⁸² See **SUBPOENAS**.

⁷⁶ 45 C.F.R. § 164.512(a); RCW 70.02.050(2)(a).

⁷⁷ 45 C.F.R. § 164.512(a); RCW 70.02.050(2)(b).

⁷⁸ RCW 70.02.050(2)(c).

⁷⁹ *Id.*

⁸⁰ *Id.*

⁸¹ 45 C.F.R. § 164.512(g); RCW 70.02.050(2)(d).

⁸² 45 C.F.R. § 164.512(e)(ii); RCW 70.02.050(2)(e).

How must a physician respond to a patient's request to examine or copy his or her own medical records?

A physician must respond to a patient's written request to examine or copy his or her records no later than 15 working days after the written request is received.⁸³ If the request is made orally, the physician must respond within 30 days of the oral request unless the information is not maintained or accessible on site, in which case the physician must respond within 60 days of the oral request.⁸⁴ A physician may require requests for access or copies of records to be made in writing as long as the physician informs patients of the requirement in advance, such as by including notice of this requirement in the physician's Notice of Privacy Practices.⁸⁵

In responding to a request to examine or copy records, the physician must do one of the following:⁸⁶

- Make the information available for examination during regular business hours and provide a copy, if requested, to the patient.
- Inform the patient that the information does not exist or cannot be found.
- Provide the name and address of the health care provider who maintains the patient's records if the health care provider receiving the request from the patient does not maintain the records.
- Specify in writing the reasons why handling the request will be delayed and the earliest date on which the information will be available for examination or copying. When responding to a written request, that date may not be later than 21 working days after receiving the written request for examination or copying. When responding to an oral request, where the delay is for any reason other than the fact that the information is not maintained or accessible on site, the physician may extend the time for response by 30 days provided the physician provides the written explanation for the delay within the initial 30-day period for response.
- Deny the request or any part of the request and inform the patient.

If the patient requests, the physician must provide an explanation of any code or abbreviation used in the health care information.⁸⁷

A physician is not required to create a new record or reformulate an existing record in order to respond to a patient's request to examine or copy his or her own records.⁸⁸

⁸³ RCW 70.02.080(1).

⁸⁴ 45 C.F.R. § 164.524(b)(2).

⁸⁵ 45 C.F.R. § 164.524(c)(4); RCW 70.02.030(2).

⁸⁶ RCW 70.02.080(1); 45 C.F.R. § 164.524(d).

⁸⁷ RCW 70.02.080(2).

⁸⁸ *Id.*

When may a physician deny a patient access to his or her medical records?

Under the UHCIA, a physician may deny access to health care information to a patient if:⁸⁹

- Knowledge of the health care information would be injurious to the health of the patient.
- Knowledge of the health care information could reasonably be expected to allow a patient to identify an individual who provided the information in confidence under circumstances in which confidentiality was appropriate.
- Knowledge of the health care information could be expected to cause danger to the life or safety of any individual.
- The health care information was compiled and used solely for litigation, quality assurance, peer review, or administrative purposes.
- Access to the health care information is otherwise prohibited by law.

Under HIPAA, a patient does not have a right of access to inspect and obtain a copy of psychotherapy notes.⁹⁰ Washington State law also places restrictions on disclosure of mental health records.⁹¹

What must a physician do if the physician denies a patient's request to examine or copy the patient's medical record?

If a physician denies a request for examination and copying of any portion of the patient's health care information, the physician must, to the extent possible, segregate out the health care information for which access was denied and permit the patient to examine or copy the rest.⁹²

If examination or copying of health care information is denied because it would be injurious to the health of the patient or because it would cause danger to the life or safety of another individual, the physician must inform the patient that the patient has a right to select another health care provider, who is licensed to treat the patient for the same condition, to review the information. If the patient selects another qualified provider to review the record, the physician must provide the information to that health care provider.⁹³

The physician must provide a written statement advising the patient of the basis of the denial, the right to have the denial reviewed, how to have the denial reviewed, and how to make

⁸⁹ RCW 70.02.090(1).

⁹⁰ 45 C.F.R. § 164.524(a)(1)(i).

⁹¹ RCW 71.05.630.

⁹² 45 C.F.R. § 164.524(d); RCW 70.02.090(2).

⁹³ 45 C.F.R. § 164.524(d)(4); RCW 70.02.090(3).

a complaint to the physician or to the Secretary of Health and Human Services, including the name or description of the contact person and phone number.⁹⁴

May a physician charge for responding to a patient's request or a subpoena for copies of the patient's medical record?

Yes. A physician may charge a reasonable cost-based fee including only the cost of supplies for and labor of copying, not to exceed actual cost, and postage (if the patient has requested the records be mailed, for responding to a patient's request or a subpoena for copies of the patient's medical record.⁹⁵ Under Washington State law, effective through June 30, 2015, such "reasonable fee" may include a clerical fee not to exceed \$24.00 for searching and handling the records, labor, and copying charges not to exceed \$1.09 per page for the first 30 pages, and \$0.82 per page for additional pages.⁹⁶ These maximum charges are subject to adjustment by the Secretary of Health every two years. A physician is not required to permit examination or copying until the fee is paid. Retail sales tax should be collected if a fee is charged for the release of records. Finally, if the party requesting the records requests or agrees to receive in lieu of the records an explanation or summary, and the individual agrees in advance, the physician may charge a reasonable cost-based fee for preparing the explanation or summary.⁹⁷

If editing of the records is required by statute and is done by the physician, the physician may charge a fee equal to the usual and customary charge for a basic office visit.⁹⁸

May a patient request that a physician correct or amend the patient's medical record?

Yes. A patient may request that his or her record be corrected or amended.⁹⁹

What must a physician do upon receipt of request to correct or amend a patient's record?

A physician, within 10 days of receiving a patient's written request to correct or amend the patient's record, must take one of the following five actions:¹⁰⁰

- Make the requested correction or amendment and inform the patient.
- Inform the patient that the record no longer exists or cannot be found.
- Inform the patient of the name and address of the person who maintains the record.
- Inform the patient of the reasons for delay in handling the patient's request and inform the patient, in writing, of the earliest date on which action will be taken on the patient's

⁹⁴ 45 C.F.R. § 164.524(d)(2).

⁹⁵ 45 C.F.R. § 164.524(c)(4); RCW 70.02.030(2).

⁹⁶ WAC 246-08-400.

⁹⁷ 45 C.F.R. § 164.524(c)(4)(iii).

⁹⁸ WAC 246-08-400(2)(b).

⁹⁹ 45 C.F.R. § 164.526(a); RCW 70.02.100(1).

¹⁰⁰ RCW 70.02.100(2).

request. The action must be taken not later than 21 days after receiving the written request.

- Inform the patient in writing of the physician's refusal to correct or amend the record and the patient's right to add a statement of disagreement.

If the request to correct or amend is made orally, then the physician has 60 days to take one of the following three actions:¹⁰¹

- Make the requested correction or amendment and so inform the patient.
- Inform the patient in writing, in plain language, of the physician's refusal to correct or amend the record and the patient's right to add a statement of disagreement.
- Provide the patient with a written statement explaining the reasons why the physician is unable to act within the 60 days, and the date by which the physician will respond to the request. Such new date cannot extend the time for response by more than 30 days, and the physician may have no more than one such 30-day extension.

A physician may require patients to make requests to correct or amend in writing as long as the physician informs the patient of the requirement in advance, such as by including notice of this requirement in the physician's Notice of Privacy Practices.¹⁰²

If a physician agrees to make the patient's proposed correction or amendment, what must the physician do?¹⁰³

In making a correction or amendment requested by a patient, a physician must:

- Add the amending information as part of the medical record.
- Mark the challenged entry or entries as corrected or amended and indicate where in the record the corrected or amended information may be found.
- Obtain the patient's identification of, and agreement for notification to be made to, persons with whom the amendment needs to be shared.

If a physician refuses to make the patient's proposed correction or amendment, what must the physician do?

If the physician refuses to make the patient's proposed correction or amendment, the physician must:¹⁰⁴

¹⁰¹ 45 C.F.R. § 164.526(b)(2).

¹⁰² 45 C.F.R. § 164.526(b)(1).

¹⁰³ 45 C.F.R. § 164.526(c); RCW 70.02.110(1).

¹⁰⁴ 45 C.F.R. § 164.526(d); RCW 70.02.110(2).

- Advise the patient of the right to submit a written statement disagreeing with the denial and how to file such a statement.
- Advise the patient that, if the patient does not submit a statement of disagreement, the patient may request the physician provide the patient's request for amendment or correction and the denial with any future disclosures of information that is the subject of the request for correction or amendment.
- Provide the patient with a description of how the patient may complain to the physician or to the Secretary of the Department of Health and Human Services, including the name or title and telephone of the contact person.
- Permit the patient to file as part of the medical record a concise statement of the requested correction or amendment and the reasons for it. The physician may prepare a rebuttal statement, but must provide a copy to the patient.
- Mark the challenged entry to indicate that the patient claims the entry is inaccurate or incomplete and indicate where in the record the patient's statement of disagreement may be found.

Must a physician notify anyone of a correction or amendment to, or a refusal to correct or amend a patient's medical record?

Yes. A physician must forward any change made in a health care information or medical record to a third party payor or insurer to which the physician had previously disclosed the health care information that is the subject of the patient's request to correct or amend.¹⁰⁵ The physician must also obtain the patient's identification of, and agreement to have the physician notify, relevant persons with whom the amendment needs to be shared.¹⁰⁶

What is required before a physician may respond to an attorney's discovery request or subpoena for health care information about a patient?

Under the UHCIA, an attorney must provide 14 days advance notice to the physician and to the patient or the patient's attorney, through service of process or first class mail, before the attorney may serve a discovery request or subpoena on a health care provider for health care information about a patient.¹⁰⁷ The advance notice must contain the following information:¹⁰⁸

- The name of the physician from whom the information is sought.
- What health care information is sought.

¹⁰⁵ RCW 70.02.110(3).

¹⁰⁶ 45 C.F.R. § 164.526(c)(3).

¹⁰⁷ RCW 70.02.060(1).

¹⁰⁸ *Id.*

- The date by which a protective order must be obtained to prevent the physician from complying with the discovery request or subpoena.

The advance notice provision is designed to give the patient and the physician adequate time to seek a protective order in the event they wish to limit or prevent the disclosure of health care information.

Absent written consent of the patient, a physician who receives a discovery request or subpoena from an attorney for health care information may not disclose the health care information if the attorney has not complied with the advance notice requirement.¹⁰⁹

If the attorney has complied with the advance notice requirement and no protective order has been issued by a court, the physician must disclose the requested information.¹¹⁰

If the physician complies with the discovery request or subpoena, the discovery request or subpoena must be made a part of the patient's record.¹¹¹

The notice of intent procedure under the UHCIA should satisfy the corresponding requirements under HIPAA.¹¹²

Must a physician, when releasing a record, provide a certification of record upon request?

Yes. Under the UHCIA, upon the request of the person requesting the record, a physician must certify the record and may charge a fee of \$2.00 for such certification.¹¹³ The physician need not certify the record until the fee is paid. The certification must be attached to the record and must contain:¹¹⁴

- The identity of the patient.
- The kind of health care information involved.
- The identity of the person to whom the information is being furnished.
- The identity of the physician or facility furnishing the information.
- The number of pages of the health care information.
- The date on which the health care information is furnished.
- That the certification is to fulfill and meet the certification requirements of the UHCIA.

¹⁰⁹ RCW 70.02.060(2).

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² 45 C.F.R. § 164.512(e).

¹¹³ RCW 70.02.070; RCW 36.18.016

¹¹⁴ RCW 70.02.070.

May a physician discuss a patient with an attorney, other than the physician's own attorney, without the patient's consent?

Generally, no. A physician may not discuss a patient's health care information with an attorney, other than the physician's own attorney, without a signed patient authorization, a subpoena issued in compliance with the requirements of the UHCIA, or a court order.¹¹⁵ This general rule, however, does not apply in workers' compensation cases.¹¹⁶ See **WORKERS' COMPENSATION**.

May a physician discuss a patient with the physician's own attorney without the patient's consent?

Generally, yes. But before doing so the physician should obtain a signed HIPAA-compliant business associate agreement with the attorney.¹¹⁷

What is a business associate agreement?

A business associate agreement is a document that sets forth the obligations a business associate must meet in order to adequately protect health information the business associate may receive from the physician.¹¹⁸ Physicians are required to have business associate agreements in place with all of their business associates with whom they share patients' protected health information.¹¹⁹ Business associates are persons or entities, other than employees, who on behalf of the physician perform or assist in performing a function or activity that involves the use or disclosure of protected health information maintained by the physician. Examples of business associates include a physician's billing agent, attorney, accountant, and collection agency, but do not include the physician's employees.

A HIPAA-compliant sample business associate agreement may be found at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>.

When does a physician need to obtain a business associate agreement?

A physician needs to obtain a signed business associate agreement from every business associate with which the physician may share protected health information in order for the business associate to perform or assist in performing a function on behalf of the physician.¹²⁰ The new changes have expanded the kinds of entities that are considered business associates, and make business associates liable for certain HIPAA violations. Where provided, the standards, requirements, and implementation specifications of the HIPAA Privacy, Security, and Breach Notification Rules also apply to business associates, not just the covered entity.¹²¹ Any person or

¹¹⁵ RCW 70.02.060(2).

¹¹⁶ RCW 51.36.060.

¹¹⁷ 45 C.F.R. § 164.502(e)(1).

¹¹⁸ 45 C.F.R. § 164.504(e).

¹¹⁹ 45 C.F.R. § 164.502(e)(2).

¹²⁰ 45 C.F.R. § 164.502(e)(2).

¹²¹ 45 C.F.R. § 164.104(b).

entity (other than a member of the covered entity's workforce) who creates, receives, maintains, or transmits PHI on behalf of the covered entity is considered a business associate.¹²² The new changes have added the word "maintains" to the definition, so that entities that never or infrequently view the PHI they maintain are still responsible for its security. This will include subcontractors who create, receive, maintain or transmit PHI on behalf of a business associate.¹²³ Covered entities are not required to enter into Business Associate Agreements with subcontractors, but the business associate *is* required to do so.

Under the UHCIA, what type of notice regarding medical record disclosure must be made to patients?

Under the UHCIA, physicians must provide notice to patients stating substantially the following:¹²⁴

"We keep a record of the health care services we provide you. You may ask us to see and copy that record. You may also ask us to correct that record. We will not disclose your record to others unless you direct us to do so or unless the law authorizes or compels us to do so. You may see your record or get more information about it at _____."

This notice must be given by posting it in a conspicuous place, including it on a consent form, providing it with billing or otherwise directly sending it to patients.¹²⁵

Under HIPAA, what type of notice regarding disclosure of health care information must be given to patients?

Under HIPAA, a physician must provide each patient, no later than the first date of service or, in the case of emergency, as soon as practicable, with a copy of the physician's Notice of Privacy Practices, and should obtain an acknowledgment of receipt.¹²⁶ The Notice of Privacy Practices must also be posted in a clear and prominent location, and a copy must be made available on request.¹²⁷ Whenever the Notice of Privacy Practices is revised, a copy of the new notice must be made available in the physician's office.¹²⁸

The Notice of Privacy Practices must be written in plain language and is to provide notice to patients of the uses and disclosures of protected health information that may be made by the physician and of the patient's rights and the physician's legal duties with respect to protected health information.¹²⁹ As of September 23, 2013, providers are required to expand what is

¹²² 45 C.F.R. §160.103.

¹²³ *Id.*

¹²⁴ RCW 70.02.120(1).

¹²⁵ RCW 70.02.120(2).

¹²⁶ 45 C.F.R. § 164.520(c)(2).

¹²⁷ 45 C.F.R. § 164.520(c)(2)(iii).

¹²⁸ 45 C.F.R. § 164.520(c)(2)(iv).

¹²⁹ 45 C.F.R. § 164.520(b)(1).

included in the Notice of Privacy Practices provided to their patients.¹³⁰ Notices must now clearly explain patients' rights to restrict disclosures, the type of disclosures that would require a patient's authorization (see answer to the question "*When must a provider get the patient to authorize the use and disclosure of PHI?*" below), and their rights as individual patients to opt out of certain communications (see answer to the question "*Can a provider use patient information for fundraising purposes?*" immediately below).¹³¹ The notice must contain a statement briefly explaining the individual's rights, and the patient's ability to request restrictions on certain uses and disclosures of PHI.¹³²

Additionally, the covered entity must now inform patients about their rights to notice if there is an information breach, as well as their rights regarding the use of their genetic information for health plan underwriting purposes.¹³³ In addition to these new requirements, HIPAA sets forth a very long list of items that must be included in the Notice of Privacy Practices that are too detailed to be included in this Guide.¹³⁴ September 23, 2013 is the deadline by which covered entities must be in compliance with these new requirements, or else risk facing patient complaints, governmental investigations, and civil and criminal penalties.¹³⁵ For assistance in preparing a plain language Notice of Privacy Practices, please go to <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/notice.html>.

Can a provider use patient information for fundraising purposes?

There are six categories of health information that may be used and disclosed for the purpose of fundraising, even without a patient's prior consent. This includes:¹³⁶

- Patient demographic information
- Health insurance status
- Dates of patient health care services
- General department of service information
- Treating physician information
- Outcome information

Despite this, patients must still be given the ability to "opt out" of fundraising. Providers must either tell or provide in writing an explanation of the patient's right to opt out¹³⁷ that:

¹³⁰ 78 FR 5566 (Jan. 25, 2013); 45 C.F.R. §164.520(b)(iii)(A).

¹³¹ 45 C.F.R. § 164.520.

¹³² 45 C.F.R. §164.520(b)(iv).

¹³³ *Id.*

¹³⁴ *Id.*

¹³⁵ 42 U.S.C. § 1320d-6 (2000).

¹³⁶ 45 C.F.R. § 164.514(f)(1).

¹³⁷ 45 C.F.R. §164.520 (b)(iii)(A).

- Is clear, written in plain language, and a conspicuous part of the materials provided to the patient; and
- Describes a simple way for the patient to opt out from receiving any other fundraising materials from the provider.

When must a provider get the patient to authorize the use and disclosure of PHI?

Generally, except as otherwise permitted or required by this statute, a covered entity may not use or disclose PHI without a valid authorization. When a covered entity obtains or receives an authorization for the use or disclosure of PHI, the covered entity can only use or disclose the PHI in a manner consistent with the authorization. Additionally, the following require specific authorizations:

- The use or disclosure of psychotherapy notes¹³⁸
- The use or disclosure of PHI for marketing, except in specific situations permitted by the statute¹³⁹
- The sale of PHI¹⁴⁰

What may happen if a physician fails to comply with requirements of the UHCIA?

If a physician fails to comply with UHCIA requirements, a patient may bring a lawsuit against a physician who fails to comply with the requirements of the UHCIA.¹⁴¹ In such a lawsuit, the patient may obtain a court order compelling the physician to comply with the law and may recover any actual damages sustained as a result of the physician's failure to comply with the law.¹⁴² If the patient prevails, the patient may also recover reasonable attorneys' fees and expenses incurred in bringing the action.¹⁴³

What may happen if a physician fails to comply with HIPAA requirements?

If a physician fails to comply with HIPAA requirements, a patient may file a complaint with the Office for Civil Rights (OCR), who may in turn investigate the physician.¹⁴⁴ The physician must cooperate with the investigation and give the OCR access to the physician's facilities, books, and records.¹⁴⁵ If the OCR finds that the physician has violated HIPAA, it may

¹³⁸ 45 C.F.R. § 164.508(a)(2).

¹³⁹ 45 C.R.R. § 164.508(a)(3).

¹⁴⁰ 45 C.R.R. § 164.508(a)(4).

¹⁴¹ RCW 70.02.170(1).

¹⁴² RCW 70.02.170(2).

¹⁴³ *Id.*

¹⁴⁴ 45 C.F.R. § 160.305.

¹⁴⁵ 45 C.F.R. § 160.310.

impose civil monetary penalties of up to \$100 per person for each violation, and up to \$25,000 for violations of a single standard within the calendar year.¹⁴⁶

A new, four-level tiered civil money penalty structure has been created by the HITECH Act.¹⁴⁷ Penalties are now assessed depending on the covered entity's culpability;¹⁴⁸ the minimum penalty amount for each violation has been set at \$100 for each HIPAA violation, and the maximum penalty has been increased to \$1.5 million dollars annually.¹⁴⁹ Additionally, covered entities may no longer avoid monetary penalties by using the affirmative defense that they did not know (and would not have known if they had been reasonably diligent) of the violation.¹⁵⁰ Previously, the Secretary could not impose a monetary penalty if the covered entity could demonstrate that it did not know and could not have known of the violation, but this is no longer true.¹⁵¹

State Attorney Generals may now bring civil actions on behalf of the residents of the state, if it can be shown that the residents were harmed by a covered entity's non-compliance.¹⁵²

Criminal penalties for wrongful disclosure of protected health information can also be imposed which, upon conviction, could result in fines of up to \$50,000 and imprisonment for up to one year, or both.¹⁵³ For criminal offenses involving conduct, the possible penalties include fines of up to \$250,000 and imprisonment for up to 10 years.¹⁵⁴

Does the UHCIA supersede all other special rules governing disclosure of health care information?

No. In particular, the UHCIA does not alter the terms and conditions of disclosure of health care information contained in statutes and regulations governing workers' compensation, control and treatment of sexually transmitted diseases, mental health treatment, drug and alcohol abuse treatment, juvenile justice, or marital dissolutions.¹⁵⁵

Under the UHCIA, how long must a physician maintain a record of existing health care information following receipt of a valid patient authorization?

Under the UHCIA, a record of existing health care information must be maintained for at least one year following receipt of a valid patient authorization, and during the pendency of a request for examination and copying or a request for correction or amendment.¹⁵⁶ See also **RETENTION OF RECORDS.**

¹⁴⁶ 45 C.F.R. § 160.404.

¹⁴⁷ HITECH Act § 1310(d), codified at 42 U.S.C. § 1176(a). See also 45 C.F.R. §§ 160.404, 160.406, 160.408.

¹⁴⁸ HITECH Act § 13410(d)(1)(C)(ii); codified at 42 U.S.C. § 17939(d)(1)(C)(ii). See also 45 C.F.R. § 160.404(b).

¹⁴⁹ HITECH Act § 13410 (d)(1)(C)(ii); codified at 42 U.S.C. § 17939(d)(1)(C)(ii). See also 45 C.F.R. § 160.404(b).

¹⁵⁰ HITECH Act § 13410(d)(4); codified at 42 U.S.C. § 1176(b).

¹⁵¹ *Id.* See also 45 C.F.R. § 160.410(b)(2).

¹⁵² HITECH Act §§ 13410(e); 42 U.S.C. § 17939(e).

¹⁵³ 42 U.S.C. § 1320d-6(b)(1).

¹⁵⁴ 42 U.S.C. § 1320d-6(b)(2)- (3).

¹⁵⁵ RCW 70.02.900.

¹⁵⁶ RCW 70.02.160.

Under HIPAA, how long must a physician maintain sufficient information to respond to a patient's request for an accounting?

HIPAA requires a physician to maintain sufficient information to respond to a patient's request for an accounting of disclosures made during the six years preceding the request.¹⁵⁷

What safeguards must physicians take to protect health care information?

Physicians must take reasonable safeguards to ensure the confidentiality, integrity and availability of health care information they maintain.¹⁵⁸ HIPAA's Security Rule also imposes a wide range of obligations for maintaining the security of health care information which are beyond the scope of this Guide.¹⁵⁹

Are there specific safeguards related to telephone or facsimile numbers that must be taken for the security of health care information?

Yes, action must be taken to delete outdated and incorrect facsimile or other telephone numbers from computers, facsimile machines, or other databases.¹⁶⁰ When transmitting health care information by facsimile to a recipient that is not regularly sent such information, the physician must verify that the number is accurate before transmitting the information.¹⁶¹

Where can more detailed information about the federal privacy and security regulations under HIPAA be obtained?

More information about the HIPAA Privacy and Security Rules and related regulations may be obtained from the following web site: <http://www.hhs.gov/ocr/hipaa>.

¹⁵⁷ 45 C.F.R. § 164.528(a).

¹⁵⁸ RCW 70.02.150.

¹⁵⁹ 45 C.F.R. Part 160, Part 164, Subparts A and C.

¹⁶⁰ RCW 70.02.150.

¹⁶¹ *Id.*