

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

This checklist is intended to assist your organization in assessing its readiness to comply with the Administrative Simplification standards contained in the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) that relate to privacy of protected health information (“Privacy Rule”). HIPAA’s Administrative Simplification standards relating to transactions and code sets and unique identifiers (“TCS Rule”) are addressed in a separate checklist. The Security Rule, including the standard for electronic signatures, is still in the proposal stage. You will find a brief description of the proposed Security Rule in this document; a checklist for that rule will be provided at a later date.

Completion of the checklists is one method of documenting your organization’s HIPAA compliance efforts. We strongly recommend that you keep a file copy of each checklist after it has been completed.

For additional HIPAA information and answers to FAQs, you may wish to consult the following websites: <http://www.cms.hss.gov/hipaa/hipaa2/default.asp>, and <http://www.hipaadvisory.com>.

The compliance date for the HIPAA Privacy Rule is April 14, 2003.

DISCLAIMER: These checklists are intended only for use as an aid to your organization in assessing its compliance with the HIPAA Administrative Simplification standards. Notices of Proposed Rulemaking (“NPRM”) may be issued that change the scope and content of the standards on which the checklists are based. The checklists do not take into account any state or federal requirements that, if applicable to your organization now, will continue to be applicable (e.g., the federal requirements contained in 42 CFR §§ 59.11 (Title X Grantee Confidentiality) and 51c.110 (§ 330 Grantee Confidentiality), nor have they been tailored to any individual organization’s specific needs or requirements. Use of the Checklists will neither assure that any individual organization is compliant with HIPAA nor constitute certification of HIPAA compliance.

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Privacy Rule. A summary of the Privacy Rule and its purposes is set forth below. This summary has been updated to reflect the changes to the Rule that are effective October 15, 2002.

As described in the HHS Fact Sheet issued by the United States Department of Health and Human Services (“DHHS”) on January 22, 2002, the Privacy Rule “limits the use and release of individually identifiable health information; gives patients the right to access their medical records; restricts most disclosure of health information to the minimum needed for the intended purpose; and establishes safeguards and restrictions regarding disclosure of records for certain public responsibilities, such as public health, research and law enforcement. Improper uses or disclosures under the rule are subject to criminal and civil sanctions prescribed in HIPAA.”

Health care providers that are “Covered Entities” under HIPAA must comply with the Privacy Rule “with respect to protected health information.” 45 CFR § 164.500(a). Health care providers are “Covered Entities” if they “transmit any health information in electronic form in connection with a transaction” covered by HIPAA. 45 CFR § 160.102(a)(3). “Protected Health Information” (“PHI”) is defined, with certain limited exceptions, as “individually identifiable health information” that is transmitted by or maintained in electronic media or “*any other form or medium.*” 45 CFR § 164.501; emphasis added.

The Privacy Rule is extraordinarily detailed and prescriptive. In preparing the Gap Assessment Checklist for this Rule, we have tried to strike a reasonable balance, providing enough information to allow you to identify and assess your organization’s general level of compliance with the Privacy Rule’s requirements, but without setting forth every caveat and exception set forth in the Rule. To aid you in obtaining additional information regarding the items listed on the Checklist, we have provided, where applicable, citations to the Privacy Rule from which the Checklist elements were derived. In addition, where it seemed useful and was not voluminous, we have provided explanatory notes regarding the Privacy Rule’s requirements.

The date by which organizations covered by the Privacy Rule must comply with the Rule is April 14, 2003.

Security Rule and Standard for Electronic Signatures. Closely allied to the Privacy Rule is the rule related to security of health information. On August 12, 1998, DHHS published an NPRM to set standards both for security of health information, whether individually identifiable or not, as well as a standard for electronic signatures. The Security Rule proposes to establish security measures for administrative procedures, physical safeguards, technical security services, and technical security mechanisms. In the NPRM, DHHS describes the Security Rule as follows:

In this proposed rule, we propose a standard for security of health information. This rule would establish that health plans, health care clearinghouses, and health care providers must have the security standard in place to comply with the statutory requirement that health care information and individually identifiable health care information be protected to ensure privacy and confidentiality when health information is electronically stored, maintained, or transmitted. The Congress mandated a separate standard for electronic signature, therefore, this proposed security standard also addresses the selected standard for electronic signature. The proposed security standard does not require the use of an electronic signature, but specifies the standard for an electronic signature that must be followed if such a signature is used. If an entity elects to use an electronic signature, it must comply with the electronic signature standard.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Privacy Rule: Applicability

	Yes	No
Is your organization a health care provider that transmits any health information in electronic form in connection with a transaction covered by the HIPAA Administrative Simplification Rules? (If so, your organization is a Covered Entity under HIPAA.) ^(45 CFR § 160.102)		
Does your organization bill Medicare? (If so, even if your organization conducts no other HIPAA-covered transactions electronically, it will be required to submit claims to Medicare electronically by October 16, 2003 and will become a Covered Entity.)		
Does your organization transmit by or maintain in electronic media or any other form or medium any individually identifiable information as defined below? (If so, the information is protected health information ("PHI"), and the Privacy Rule applies with respect to such PHI.) ^{1 (45 CFR § 164.501)}		
<ul style="list-style-type: none"> • health information, including demographic information collected from the individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and 		
<ul style="list-style-type: none"> • 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 health care to an individual; and 		
<ul style="list-style-type: none"> • that identifies the individual to which the health information pertains or can be used to identify that individual. 		

Notes

1. *The Privacy Rule excludes certain types of individually identifiable health information from the definition of PHI, including that in education records covered by FERPA, student records as defined in FERPA, and employment records held by a Covered Entity in its role as employer. (45 CFR § 164.501)*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Privacy Rule: Preliminary Information & Designations

	Yes	No
Has your organization identified a HIPAA Compliance Committee for implementation of HIPAA requirements? ¹		
Has the Committee developed a work plan, timetable, and budget for implementation of the Privacy Rule?		
Has the Committee identified and inventoried all of the organization's systems and applications that contain PHI? ²		
Has the Committee identified and inventoried all departments, employees, and vendors with access to PHI?		
Has the Committee identified, collected, and inventoried all policies and procedures ("P&Ps"), practices, and other documents relating to PHI? ³		
Has the Committee identified, collected, and inventoried all written and oral agreements between your organization and other entities or individuals that have access to PHI? ⁴		
Has the Committee identified, collected, and inventoried all P&Ps and practices regarding the physical and technical security of PHI? ⁵		

Notes

1. *This might include representatives of affected functions as well as those with legal compliance, MIS, information security, and physical security capabilities.*
2. *This will need to include inventorying of systems and applications of vendors the organization uses that contain PHI.*
3. *Documents other than P&Ps might include informed consents, as well as all consents, authorizations, releases, and other similar documents relating to the use and disclosure of PHI.*
4. *These will include both contractual and unwritten arrangements with employees, consultants, and vendors that have access to PHI.*
5. *Requirements related to security of PHI are to be covered in more depth in the Security Rule. As noted above, the Security Rule is not yet in final form. Please note, however, that the Security Rule requirements apply not only to PHI, but to all health information, as that term is defined under HIPAA. Accordingly, you may wish to expand the scope of your organization's preliminary information gathering to include not only that related to PHI, but also that related to health information generally.*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

U/D of PHI: General Requirements

	Yes	No
Is your organization's use and disclosure ("U/D") of PHI in accordance with the general requirements of the Privacy Rule set forth below? ¹ (45 CFR § 164.502(a))		
Does your organization only U/D the minimum necessary PHI to accomplish the intended purpose of the U/D? ² (45 CFR § 164.502(b))		
Does your organization's U/D of PHI comply with any restrictions on U/D to which your organization has agreed? ³ (45 CFR § 164.502(c))		
Does your organization comply with Privacy Rule requirements relating to de- and re-identified health information? ⁴ (45 CFR § 164.502(d))		
Does your organization comply with the Privacy Rule with respect to the PHI of the deceased? ^{(45 CFR § 164.502(f))}		
Does your organization treat personal representatives of the patient appropriately under the Privacy Rule? ⁵ (45 CFR § 164.502(g))		
Are all U/Ds by your organization consistent with your organization's Notice of Privacy Practices? ⁶ (45 CFR § 164.502(i))		

Notes

1. *The Privacy Rule's requirements regarding U/D of PHI on optional consent, authorization, and without consent and authorization, as well as those regarding Business Associates and the right to confidential communications, are addressed in subsequent sections, below. Also, 45 CFR § 164.502(j) contains an exception to these requirements for whistle blowers and workforce members who are crime victims, so long as certain conditions are met.*
2. *The minimum necessary requirement is not applicable in all instances. For example, this requirement does not apply to disclosures to or requests by a health care provider for treatment, U/D to the individual, U/D pursuant to an authorization, disclosures to DHHS, U/D required by law, and U/D for compliance with the Privacy Rule. See also, "U/D of PHI: Minimum Necessary," below.*
3. *See also "Right to Request Restrictions on U/D of PHI," below.*
4. *See also "U/D of PHI: De-Identification of PHI," below. Health information that has been de-identified in compliance with the Privacy Rule is not subject to the Rule.*
5. *The Privacy Rule contains extensive implementation specifications regarding the treatment of representatives of adults, emancipated and unemancipated minors, and the deceased, and in abuse, neglect, and endangerment situations.*
6. *See also "Notice of Privacy Practices," below.*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

U/D of PHI: Business Associates

	Yes	No
Does your organization use individuals and entities not part of the workforce to perform any of the functions or activities or provide any of the services described in the definition of business associates? (If so, your organization must comply with the provisions of the Privacy Rule relating to business associates.) ¹ (45 CFR §§ 160.103 and 164.502(e))		
Are all such arrangements with business associates reduced to a writing that is compliant with the Privacy Rule? ² (45 CFR §§ 164.502(e)(2) & 164.504(e))		
Does your organization have a procedure in place by which it takes reasonable steps to cure or end violations of its arrangements with business associates that is compliant with the Privacy Rule? ⁽⁴⁵ CFR § 164.504(e)(i)-(ii))		

Notes

1. *Business Associates are individuals and entities not part of your organization’s workforce that, on your organization’s behalf (i) perform functions or activities that involve the use or disclosure of individually identifiable health information such as claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing; (ii) perform functions or activities regulated by the HIPAA Administrative Simplification Rules; or (iii) provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services where provision of the service involves disclosure of individually identifiable health information to the business associate. Disclosures by a Covered Entity to a health care provider concerning the treatment of an individual are not subject to the business associate requirements set forth in the Privacy Rule.*
2. *The Privacy Rule contains a number of requirements regarding the content of such contracts and other arrangements with business associates. Federal Register, Vol. 67, No. 157 (8/14/02) contains sample business associate contract provisions in an appendix to the preamble.*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

U/D of PHI: Optional Consent

	Yes	No
Does your organization limit its U/D of PHI to carry out treatment, payment, and health care operations ("TPO") on "optional consent" to the TPO categories listed below? ¹ (45 CFR § 164.506)		
Is the U/D of PHI for your organization's own treatment, payment, or health care operations? (45 CFR § 164.506(c)(1))		
Is the disclosure of PHI for treatment activities of a health care provider? (45 CFR § 164.506(c)(2))		
Is the disclosure of PHI to another Covered Entity or a health care provider for the payment activities of the entity that receives the information? (45 CFR § 164.506(c)(3))		
Is the disclosure of PHI to another Covered Entity for health operations activities of the other Covered Entity under the conditions specified in the Privacy Rule? ² (45 CFR § 164.506(c)(4))		

Notes

1. *While the Privacy Rule no longer requires a consent for the U/D of PHI for TPO specified in the Privacy Rule, other federal requirements, such as those under 42 CFR §§ 59.11 (Title X Grantee Confidentiality) and 51c.110 (§ 330 Grantee Confidentiality), and/or more stringent state laws that survive HIPAA, may be applicable to your organization. Also, Privacy Rule requirements regarding U/D of psychotherapy notes and of PHI for marketing are more restrictive than for other U/Ds (see "U/D of PHI: Written Authorization," below).*
2. *Each entity must have or have had a relationship with the individual who is the subject of the PHI, the PHI must pertain to that relationship, and the purpose of the disclosure must be either for health care fraud and abuse detection or compliance or as set forth in 45 CFR §§ 164.506(1) or (2).*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

U/D of PHI: Written Authorization

	Yes	No
Is a written authorization that contains the elements listed below obtained for U/D of PHI where an authorization is required by the Privacy Rule? ¹ (45 CFR § 164.508)		
Is a written authorization obtained for U/D of psychotherapy notes? ² (45 CFR § 164.508(a)(2))		
Is a written authorization obtained for U/D of PHI for marketing? ² (45 CFR § 164.508(a)(3))		
Does the written authorization contain a specific and meaningful description of the PHI to be U/D? (45 CFR § 164.508(c)(1)(i))		
Does the written authorization specifically identify the person authorized to make the requested U/D? (45 CFR § 164.508(c)(1)(ii))		
Does the written authorization specifically identify the person to whom the requested U/D may be made? (45 CFR § 164.508(c)(1)(iii))		
Does the written authorization describe each purpose of the U/D? (45 CFR § 164.508(c)(1)(iv))		
Does the written authorization contain an expiration date or event that relates to the individual or the purpose of the U/D? (45 CFR § 164.508(c)(1)(v))		
Does the authorization contain a statement of the individual's right to revoke the authorization, the exceptions to that right, and the procedure for exercising it? (45 CFR § 164.508(c)(2)(i))		
Does the authorization contain a statement that your organization may not condition treatment, payment, enrollment or eligibility for benefits on the individual's agreement to sign the authorization? ³ (45 CFR § 164.508(c)(2)(ii))		
Does the written authorization contain a statement that the PHI U/D by the authorization may be subject to redisclosure and no longer protected by the Privacy Rule? (45 CFR § 164.508(c)(2)(iii))		
Does the written authorization contain the signature of the individual and the date the authorization was signed? (45 CFR § 164.508(c)(1)(vi))		
If signed by the individual's personal representative, does the written authorization contain a description of that person's authority to act? (45 CFR § 164.508(c)(1)(vi))		
Is the authorization written in plain language? (45 CFR § 164.508(c)(3))		
Does your organization give the individual a signed copy of any authorization that it seeks from the individual? (45 CFR § 164.508(4))		

Notes

1. *The questions in this section of the Checklist do not address Privacy Rule requirements regarding defective authorizations, compound authorizations, and the prohibition on conditioning of authorizations.*
2. *U/D of psychotherapy notes and U/D of PHI for marketing without an authorization is permissible only under certain Rule-specified circumstances.*
3. *Covered Entities may condition an authorization under certain Rule-specified circumstances; if so, the authorization must state what those circumstances are. (45 CFR §§ 164.508(b)(4) and (c)(2)(ii))*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

U/D of PHI: w/o Optional Consent or Authorization (Opportunity to Agree/Object)

	Yes	No
Are the requirements of the Privacy Rule met in all instances below that apply to your organization? (For all such instances, so long as the requirements of the Rule are met, an opportunity must be given to the individual to agree or object, but no authorization is required.) ¹ (45 CFR § 164.510)		
Is the individual informed, either orally or in writing, in advance of the U/D of PHI? (45 CFR § 164.510)		
Is the individual given the opportunity, either orally or in writing, to agree, prohibit, or restrict U/D? (45 CFR § 164.510)		
Is the use for your organization's directory, and is it limited to the PHI specified in the Privacy Rule? ² (45 CFR § 164.510(a)(1)(i))		
Is religious affiliation contained in the directory disclosed only to the clergy and is other directory information only disclosed to persons who ask for the individual by name? (45 CFR § 164.510(a)(1)(ii))		
Is the disclosure for involvement in the individual's care or payment for care? ³ (45 CFR § 164.510(b)(1)(i))		
Is the U/D for notification to a family member, a personal representative, or other person responsible for the individual's care, and is it restricted to notification of the person's location, general condition, or death? (45 CFR § 164.510(b)(1)(ii))		
Is the U/D for disaster relief purposes? (45 CFR § 164.510(b)(4))		

Notes

1. *While the Privacy Rule requires no consent or authorization for these U/D of PHI, other federal requirements, such as those under 42 CFR §§ 59.11 (Title X Grantee Confidentiality) and 51c.110 (§ 330 Grantee Confidentiality), and/or more stringent state laws that survive HIPAA, may be applicable to your organization.*
2. *The use of PHI must be limited to name, location in facility, condition in general terms, and religion; the opportunity to object may not apply in emergency circumstances.*
3. *The disclosure may be made only to a family member, a relative, a close friend, or another person the individual identifies and must be relevant to that person's involvement in the individual's care or payment for that care.*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

U/D of PHI: w/o Optional Consent or Authorization (No Opportunity to Agree/Object)

Are the requirements of the Privacy Rule met in all instances below that apply to your organization? (For these instances, the Rule requires no opportunity to agree or object and no authorization.) 1 (45 CFR § 164.512)		
Is the U/D required by law? (45 CFR § 164.512(a))		
Is the disclosure for public health activities? (45 CFR § 164.512(b))		
Is the disclosure about victims of abuse, neglect, or domestic violence? (45 CFR § 164.512(c))		
Is the disclosure for health oversight activities? (45 CFR § 164.512(d))		
Is the disclosure for a judicial or administrative proceeding? (45 CFR § 164.512(e))		
Is the disclosure for law enforcement purposes? (45 CFR § 164.512(f))		
Is the disclosure to a coroner, medical examiner, or funeral director about a decedent? (45 CFR § 164.512(g))		
Is the U/D for cadaveric organ, eye, or tissue donation purposes? (45 CFR § 164.512(h))		
Is the U/D for research purposes and compliant with Rule-mandated conditions? (45 CFR § 164.512(i))		
Is the U/D to avert a serious threat to health or safety? (45 CFR § 164.512(j))		
Is the U/D for a specialized government function set forth in the Privacy Rule? 2 (45 CFR § 164.512(k))		
Is the disclosure for workers' compensation or another similar program? 3 (45 CFR § 164.512(l))		

Notes

1. While the Privacy Rule requires no consent or authorization for these U/D of PHI, other federal requirements, such as those under 42 CFR §§ 59.11 (Title X Grantee Confidentiality) and 51c.110 (§ 330 Grantee Confidentiality), and/or more stringent state laws that survive HIPAA, may be applicable to your organization.
2. These include, for example, military, veteran, correctional institutions, and other specialized government functions.
3. The program must be established by law and provide benefits for work-related injuries or illness without regard to fault.

U/D of PHI: De-Identification of PHI

	Yes	No
Does your organization follow the Privacy Rule requirements for de- and re-identification of PHI? 1 (45 CFR § 164.514(a)-(c))		

Notes

1. The Privacy Rule contains several specific implementation requirements regarding de- and re-identification of PHI. Properly de-identified health information is not PHI, and is therefore not subject to the Rule.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

U/D of PHI: Minimum Necessary

	Yes	No
Does your organization meet the "minimum necessary" requirements set forth below regarding U/D of PHI? (45 CFR § 164.514(d))		
Has your organization identified those members of its workforce who need access to PHI to carry out their duties? (45 CFR §164.514(d)(2)(i)(A))		
Has your organization identified the category(ies) of PHI to which such workforce members need access? (45 CFR §164.514(d)(2)(i)(B))		
Has your organization identified the conditions, if any, under which such workforce members can gain access to such PHI? (45 CFR §164.514(d)(2)(i)(B))		
Does your organization make reasonable efforts to limit the access of identified categories of workforce members to PHI to the conditions specified by your organization? (45 CFR § 164.514(d)(2)(ii))		
For all disclosures made on a routine and recurring basis, has your organization implemented P&Ps that limit the PHI disclosed to that reasonably necessary to achieve the disclosure's purpose? 1 (45 CFR § 164.514(d)(3)(i))		
For all disclosures not made on a routine and recurring basis, does your organization have criteria for limiting the PHI to that reasonably necessary to achieve the disclosure's purpose? 1 (45 CFR § 164.514(d)(3)(ii)(A))		
For all disclosures not made on a routine and recurring basis, does your organization review the request for disclosure on an individual basis in accordance with its criteria? 1 (45 CFR § 164.514(d)(3)(ii)(B))		
Does your organization limit its own requests for disclosure of PHI to other Covered Entities to those that are reasonably necessary to the request's purpose? (45 CFR § 164.514(d)(4)(i))		
For all requests for disclosure of PHI your organization makes on a routine and recurring basis, has your organization implemented P&Ps that limit such requests to the PHI reasonably necessary to achieve the request's purpose? (45 CFR § 164.514(d)(4)(ii))		
For all requests for disclosure of PHI your organization makes that are not made on a routine and recurring basis, does your organization have criteria for limiting the PHI to that reasonably necessary to achieve the purpose of the request? (45 CFR § 164.514(d)(4)(iii)(A))		
Does your organization review all requests for PHI your organization makes that are not made on a routine and recurring basis to determine that the PHI sought is reasonably necessary to achieve its purpose? (45 CFR § 164.514(d)(4)(iii)(B))		
Does your organization refrain from using, disclosing, or requesting an entire medical record, except when the entire record is specifically justified as the amount reasonably necessary to accomplish the purpose of the use, disclosure, or request? (45 CFR 164.514(d)(5))		

Notes

- In certain instances, the organization may rely on another's representation that the PHI requested is minimally necessary. (45 CFR § 164.514 (d)(3)(iii))*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

U/D of PHI: Limited Data Sets

	Yes	No
Does your organization U/D limited data sets in accordance with the Privacy Rule requirements listed below? ¹ (45 CFR § 164.514(e))		
Does your organization U/D limited data sets only for the purposes of research, public health, or health care operations? (45 CFR § 164.514(3)(i))		
Does your organization have a data use agreement with each limited data set recipient that meets the requirements of the Privacy Rule? (45 CFR § 164.514(e)(4)(i)-(ii))		
Does your organization have a procedure in place by which it takes reasonable steps to cure or end violations of its arrangements with limited data set recipients that is compliant with the Privacy Rule? (45 CFR § 164.514(e)(iii))		

Notes

- A limited data set is PHI that excludes certain Privacy Rule-specified direct identifiers of the individual, relatives, employers, or household members of the individual. (45 CFR § 164.514(e)(2))*

U/D of PHI: Fundraising

	Yes	No
Does all U/D of PHI for fundraising that your organization conducts that is not pursuant to an authorization meet the following requirements? (45 CFR § 164.514(f))		
Is the U/D to a business associate or an institutionally related foundation for the purposes of raising funds for your organization's own benefit?		
Is the PHI limited to demographic information and dates of health care provided to an individual?		
Is the statement regarding fundraising required by the Privacy Rule included in the NPP?		
Do the fundraising materials sent to individuals contain a description of how the individual may opt out of receiving further fundraising communications?		
Does your organization make reasonable efforts to ensure that individuals who opt out do not receive further fundraising communications?		

U/D of PHI: Verification

	Yes	No
Does your organization verify all requests for disclosure of PHI in accordance with the Privacy Rule? ¹ (45 CFR § 164.514(h))		

Notes

- Subject to certain exceptions and conditions, verification includes verifying the identity and authority of the person to have access to the PHI.*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Notice of Privacy Practices

	Yes	No
Has an NPP been prepared that meets the following requirements and is otherwise compliant with the Privacy Rule? ¹ (45 CFR § 164.520)		
Is the NPP written in plain language? (45 CFR § 164.520(b)(1))		
Does the NPP contain all the regulatorily required elements? ² (45 CFR § 164.520(b)(1))		
Does the NPP contain all the optional elements applicable to your organization? ³ (45 CFR § 164.520(b)(2))		
Does your organization have a P&P for revising the NPP that is compliant with the Privacy Rule? (45 CFR § 164.520(b)(3))		
Does your organization have a P&P that is compliant with the Privacy Rule for providing the NPP to applicable individuals? ⁴ (45 CFR § 164.520(c))		
Does your organization have a P&P that is compliant with the Privacy Rule for documenting its compliance with the NPP requirements? ⁵ (45 CFR § 164.520(e))		

Notes

1. *With certain limited exceptions, individuals have a right to adequate notice of U/D of PHI. The Privacy Rule specifies in significant detail what the NPP must contain; the Checklist contains only the broad categories of requirements generally applicable to health care providers.*
2. *The required elements are listed in the Privacy Rule.*
3. *These requirements pertain if an entity elects to limit U/D that would otherwise be permitted under the Privacy Rule.*
4. *Among other requirements, health care providers with direct treatment relationships with individuals must, except in emergency treatment situations, make a good faith effort to obtain written acknowledgment of the individual's receipt of the NPP. (45 CFR § 164.520(c)(2)(ii))*
5. *This requirement includes retention of copies of NPPs issued by your organization and any written acknowledgments, as well as documentation of good faith efforts to obtain such acknowledgments. The general documentation requirements contained in the Privacy Rule also apply to NPP-related documentation. See "Administrative Requirements" related to documentation, below.*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Right to Request Restrictions on U/D of PHI

	Yes	No
Does your organization have a procedure for giving individuals the right to request restrictions on U/D of PHI that is compliant with the Privacy Rule? ¹ (45 CFR § 164.522(a)(1))		
Does your organization have a procedure that is compliant with the Privacy Rule for terminating such restrictions? ² (45 CFR § 164.522(a)(2))		
Does your organization have a Rule-compliant procedure for documenting such restrictions? ³ (45 CFR § 164.522(a)(3))		

Notes

1. *The right to restrict is limited. In addition, the organization is not required to grant the restriction, but if it does, it must comply with the applicable Privacy Rule requirements.*
2. *Certain limitations apply to the organization's right to terminate a restriction.*
3. *See "Administrative Requirements" related to documentation, below.*

Right to Confidential Communications

	Yes	No
Does your organization permit individuals to request communications related to PHI by alternative means or at alternative locations? (45 CFR §§ 164.502(h) & 164.522(b))		
Does your organization reasonably accommodate such requests from applicable individuals in a manner compliant with the Privacy Rule? ¹ (45 CFR § 164.522(b))		

Notes

1. *The Privacy Rule contains a number of requirements that health care providers must meet in implementing the right to confidential communications. Among other things, a provider may not require the individual to explain the basis of his/her request. (45 CFR § 164.522(b)(2)(iii))*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Right of Access to PHI

	Yes	No
Does your organization give individuals a right of access to inspect and obtain a copy of PHI? 1 (45 CFR § 164.524(a) & (b))		
Does your organization act on requests for access within thirty days? ² (45 CFR § 164.524(b)(2))		
Does your organization provide access in a manner that is compliant with the Privacy Rule? 3 (45 CFR § 164.524(c))		
Does your organization handle denials of access in compliance with the Privacy Rule? 4 (45 CFR § 164.524(a)(2)-(4) & (d))		
Does your organization create and retain documentation regarding access requests in compliance with the Privacy Rule? ⁵ (45 CFR § 164.524(e))		

Notes

1. *Exceptions and conditions apply to the right of access, including, for example, an exception to the right of access for psychotherapy notes.*
2. *If the PHI is not maintained or accessible on-site, the organization must act on the request within sixty days. There is also provision for obtaining an extension so long as certain conditions are met.*
3. *The Privacy Rule contains a number of requirements regarding the right of access, including requirements related to the form, time, and manner of access and the charging of fees related to access.*
4. *The Privacy Rule contains a number of requirements regarding denials, including requirements related to the content of the denial notice and the procedure for review of denials. The Rule also specifies those grounds for denial that are unreviewable.*
5. *The Privacy Rule requires that the records subject to access and the titles of the individuals or offices responsible for handling access requests must be documented. The general documentation requirements contained in the Privacy Rule also apply to documentation of the right of access requirement. See "Administrative Requirements" related to documentation, below.*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Right to Amend PHI

	Yes	No
Does your organization give individuals a right to amend PHI? ^(45 CFR § 164.526)		
Does your organization act on requests to amend within sixty days? ^{1 (45 CFR § 164.526(b)(2))}		
Does your organization have a procedure for accepting amendments that is compliant with the Privacy Rule? ^{2 (45 CFR § 164.526(c))}		
Does your organization have a procedure for denying amendments that is compliant with the Privacy Rule? ^{3 (45 CFR § 164.526(d))}		
Does your organization, when notified, amend PHI from other entities in a manner compliant with the Privacy Rule? ^{(45 CFR § 164.526(e))}		
Does your organization create and retain documentation regarding amendments in compliance with the Privacy Rule? ^{4 (45 CFR § 164.526(f))}		

Notes

1. *An extension may be obtained to this deadline if certain requirements are met.*
2. *The Privacy Rule contains specific procedural requirements regarding making the amendment, informing the individual, and informing others who have the PHI subject to the amendment.*
3. *The Privacy Rule specifies several requirements relating to such denials, including, among other things, provision of a timely written denial that contains Rule-prescribed elements and of a right to submit a statement of disagreement.*
4. *The titles of persons or offices responsible for receiving and processing requests for amendments must be documented. The general documentation requirements contained in the Privacy Rule also apply to the right to amend requirement. See "Administrative Requirements" related to documentation, below.*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Right to Accounting of Disclosures of PHI

	Yes	No
Does your organization give individuals a right to receive an accounting of disclosures of PHI that is compliant with the Privacy Rule? ¹ (45 CFR § 164.528(a))		
Does the content of each accounting include all disclosures for the time period specified by the Privacy Rule and meet the requirements set forth below? ² (45 CFR § 164.528(b))		
Does the accounting contain the date of the disclosure? (45 CFR § 164.528(b)(2)(i))		
Does the accounting contain the name, and, if known, the address, of the person/entity to whom the PHI was disclosed? (45 CFR § 164.528(b)(2)(ii))		
Does the accounting contain a brief description of the PHI disclosed? (45 CFR § 164.528(b)(2)(iii))		
Does the accounting contain a brief statement of the purpose of the disclosure? (45 CFR § 164.528(b)(2)(iv))		
Does the accounting contain an accounting of multiple disclosures, where such an accounting is allowed, that is compliant with the Privacy Rule? (45 CFR § 164.528(b)(3))		
Does your organization provide the accounting within sixty days of a request? ³ (45 CFR § 164.528(c)(1))		
Does your organization comply with the Privacy Rule regarding imposition of fees for provision of accountings? (45 CFR § 164.528(c)(2))		
Does your organization create and retain the documentation set forth below regarding accountings? ⁴ (45 CFR § 164.528(d))		
Does your organization document the information required by the Privacy Rule to be included in accountings? (45 CFR § 164.528(d)(1))		
Does your organization retain a copy of the written accounting provided to the individual? (45 CFR § 164.528(d)(2))		
Does your organization document the titles of the individuals or offices responsible for receiving and processing requests for accountings? (45 CFR § 164.528(d)(3))		

Notes

- 1. There are many exceptions to this right, including, among other things, disclosures of PHI for TPO, incidental disclosures, disclosures pursuant to an authorization, disclosures as part of a limited data set, and disclosures that occurred prior to the Privacy Rule compliance date.*
- 2. The accounting must include all disclosures not excepted from the accounting requirement that occurred during the six years, or such shorter time as the individual requests, prior to the date of the request, including disclosures to or by the organization's business associates.*
- 3. Under certain conditions, an extension may be obtained to this deadline.*
- 4. The general documentation requirements contained in the Privacy Rule also apply to documentation of accountings. See "Administrative Requirements" related to documentation, below.*

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Administrative Requirements

	Yes	No
Has your organization designated a privacy official responsible for the development and implementation of its P&Ps? (45 CFR § 164.530(a)(1)(i))		
Has your organization designated a contact person or office responsible for receiving complaints and handling questions re the NPP? (45 CFR § 164.530(a)(1)(ii))		
Has your organization trained all members of its workforce on its P&Ps with respect to PHI? (This must be done by no later than the Privacy Rule compliance date.) (45 CFR § 164.530(b)(2)(i)(A))		
Does your organization have a procedure in place by which it trains each new member of the workforce on its P&Ps with respect to PHI within a reasonable period after the hire? (45 CFR § 164.530(b)(2)(i)(B))		
Does your organization have a procedure in place by which it will, within a reasonable time after a material change to the P&Ps becomes effective, train all affected members of the workforce on the change? (45 CFR § 164.530(b)(2)(i)(C))		
Does your organization have appropriate administrative, technical, and physical safeguards to protect the privacy of PHI? (45 CFR § 164.530(e))		
Does your organization reasonably safeguard PHI to limit permitted incidental U/D? (45 CFR § 164.530(c)(ii))		
Does your organization have a process by which individuals can make complaints about its P&Ps or its compliance with P&Ps? (45 CFR § 164.530(d))		
Does your organization have and apply appropriate sanctions against workforce members who fail to comply with its P&Ps or the Privacy Rule? (45 CFR § 164.530(e))		
Does your organization mitigate known harmful effects from violations of its P&Ps and the Privacy Rule by its workforce and business associates? (45 CFR § 164.530(f))		
Does your organization refrain from intimidating or retaliatory acts against individuals and others as set forth in the Privacy Rule? (45 CFR § 164.530(g))		
Does your organization comply with the prohibition in the Privacy Rule against conditioning treatment of an individual on his or her waiver of rights under the Rule? (45 CFR § 164.530(h))		
Has your organization implemented P&Ps designed to comply with the Privacy Rule? (45 CFR § 164.530(i)(1))		
Does your organization have a procedure in place for changing its P&Ps related to U/D of PHI where required by the Privacy Rule? (45 CFR § 164.530(i)(2)-(5))		
Does your organization adhere to the documentation requirements set forth below? (45 CFR § 164.530(j))		
Does your organization maintain its privacy P&Ps in written or electronic form? (45 CFR § 164.530(j)(1)(i))		
Does your organization maintain a paper or electronic copy of all written communications required to be made by the Privacy Rule? (45 CFR § 164.530(j)(1)(ii))		
Does your organization maintain a written or electronic record of all actions, activities, and designations required to be documented by the Privacy Rule? (45 CFR § 164.530(j)(1)(iii))		
Does your organization retain all required documentation for six years from the later of the date of creation or the date when it was last in effect? (45 CFR § 164.530(j)(2))		

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

HIPAA PRIVACY RULE GAP ASSESSMENT CHECKLIST

Transition Provisions

	Yes	No
Has your organization ascertained whether it is eligible to take advantage of the Privacy Rule's transition provisions? ¹ (45 CFR § 164.532)		

Notes

- 1. These provisions allow entities the use of prior authorizations, permissions for research, and contracts with business associates that are not compliant with the Privacy Rule under certain specified circumstances.*

Continued Applicability of Other Laws

	Yes	No
Has your organization determined which federal and state laws regarding privacy of PHI will remain applicable and taken this into account in implementing the Privacy Rule? ¹ (45 CFR § 160.203)		

Notes

- 1. HIPAA states that, subject to certain exceptions, “a standard, requirement, or implementation specification adopted under [HIPAA that] is contrary to a provision of State law preempts the provision of State law.” Among the exceptions is that for state laws relating to privacy of health information that are “more stringent” than HIPAA.” In addition, the HIPAA Preamble contains an extensive discussion of the relationship between HIPAA and other federal laws, such as those under Title X and § 330, that relate to the privacy of health information.*