MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

HIPAA Omnibus Rule Reference Chart

By Dianne J. Bourque, Kimberly J. Gold, Ellen L. Janos, Julie K. Lappas, James Sasso, Kate F. Stewart, and Stephanie D. Willis

Mintz Levin is pleased to provide this section-by-section analysis of the HIPAA Omnibus Rule.

The chart lists provisions of the proposed privacy, security and enforcement rules mandated by the Health Information Technology for Electronic and Clinical Health Act ("HITECH") published in a proposed rule on July 14, 2010; the interim final enforcement rule—including HITECH's new, tiered penalty structure—published on October 30, 2009; and the interim final breach notification rule published pursuant to HITECH on August 24, 2009 (collectively, "Proposed Rules") and compares them to the same regulatory provisions published on January 17, 2013 as part of the Omnibus Rule (the "Final Rule"). Note that this summary does not include revisions under the Genetic Information Nondiscrimination Act (GINA), also published in the Final Rule.

For quick reference, our chart indicates whether or not there were changes between the Proposed Rules and the Final Rule and includes commentary on certain notable provisions.

We hope that this summary will serve as a useful tool as we all begin the process of understanding new requirements under HIPAA.

REFERENCE	PROPOSED RULES	FINAL RULE	CHANGE?
Part 160 – General Administrative Requirements			
§160.101 Statutory Basis and Purpose	Adds statutory references to HITECH	Adds statutory references to HITECH	No
§ 160.102 Applicability	Makes various provisions applicable to Business Associates	Makes various provisions applicable to Business Associates	No
§ 160.103	Updates various definitions and adds new definitions.	Updates various definitions and adds new definitions.	No In this section, OCR expanded the definition of "business associate" to include business associate subcontractors and extended business associate compliance obligations to such subcontractors. OCR rejected comments that this extension was beyond the scope of its statutory authority.
§160.105 Compliance dates for implementation of new or modified standards and implementation specifications	Covered entities and business associates must comply with applicable new standards and implementation specifications no later than 180 days from the effective date.	Covered entities and business associates must comply with applicable new standards and implementation specifications no later than 180 days from the effective date.	No OCR did not grant additional time for business associate or business associate subcontractor compliance.
§160.201 Statutory basis	Adds references to HITECH	Adds references to HITECH	No
§ 160.202 Definitions	Updated to add statutory references to HITECH and to reference business associates' obligation to comply	Updated to add statutory references to HITECH and to reference business associates' obligation to comply	No
§ 160.300 Applicability	Adds reference to business associates' obligation to comply	Adds reference to business associates' obligation to comply	No This provision is significant as it imposes direct civil money penalty liability on business associates for violations of applicable HIPAA provisions.
§ 160.302 [Removed and Reserved]			
§ 160.304 Principles for achieving compliance	Adds references to business associates' obligation to cooperate with the Secretary and the Secretary's provision of technical assistance to business associates	Adds references to business associates' obligation to cooperate with the Secretary and the Secretary's provision of technical assistance to business associates	No
§160.306 Complaints to the Secretary	Adds reference to complaints against business associates. States that the Secretary *will* investigate any complaint suggesting willful neglect and may investigate any other complaint.	Adds reference to complaints against business associates. States that the Secretary *will* investigate any complaint suggesting willful neglect and may investigate any other complaint.	No

§ 160.308 Compliance reviews	Adds reference to business associates. States that the Secretary will conduct a compliance review when a preliminary review indicates willful neglect and may conduct a compliance review in any other circumstance.	Adds reference to business associates. States that the Secretary will conduct a compliance review when a preliminary review indicates willful neglect and may conduct a compliance review in any other circumstance.	No OCR decided to "retain" the policy that the 30-day cure period for violations due to willful neglect, like those not due to willful neglect, begins on the date that an entity first acquires actual or constructive knowledge of the violation and will be determined based on evidence gathered by the Department during its investigation, on a case-by-case basis.
§160.310 Responsibilities of covered entities and business associates	Adds reference to business associates' obligation to provide records and compliance reports, cooperate with the Secretary and permit access to information in connection with a complaint. Permits OCR to disclose PHI to other law enforcement agencies if permissible under the Privacy Act.	Adds reference to business associates' obligation to provide records and compliance reports, cooperate with the Secretary and permit access to information in connection with a complaint. Permits OCR to disclose PHI to other law enforcement agencies if permissible under the Privacy Act.	No OCR indicates that the revisions in this section will permit closer cooperation and coordination of enforcement with State Attorneys General.
§160.312 Secretarial action regarding complaints and compliance reviews	Adds reference to investigation and resolution of complaints regarding business associates.	Adds reference to investigation and resolution of complaints regarding business associates.	No
§ 160.316 Refraining from intimidation or retaliation	Prohibits business associates from engaging in threatening or retaliatory action against a complainant.	Prohibits business associates from engaging in threatening or retaliatory action against a complainant.	No
§160.401 Definitions	Adds reference to business associates in definitions regarding *mens rea* and provides new definition for "reasonable cause."	Adds reference to business associates in definitions regarding *mens rea* and provides new definition for "reasonable cause."	No OCR intends to publish examples and guidance of how it plans to apply the definitions of "reasonable cause," "reasonable diligence," and "willful neglect" to distinguish among the penalty tiers under § 160.404 on its web site.
§ 160.402 Basis for a civil monetary penalty	Makes business associates, as well as covered entities, liable for civil monetary penalties.	Makes business associates, as well as covered entities, liable for civil monetary penalties.	No OCR provides additional explanation of its views on agency relationships between covered entities, business associates, and their subcontractors.
§ 160.404 Amount of civil monetary penalty	Establishes new, tiered penalty scheme and applies it to business associates as well as covered entities.	Establishes new, tiered penalty scheme and applies it to business associates as well as covered entities.	No OCR states that it will not impose the maximum penalty in all cases, but will determine penalty amounts based on the nature and extent of the violation, the nature and extent of resulting harm, and other factors including the time period during which the violation occurred, the number of individuals affected and the financial condition of the covered entity.

§ 160.406 Violations of an identical requirement or prohibition	Adds reference to business associate liability for continuing violations.	Adds reference to business associate liability for continuing violations.	No
§ 160.408 Factors considered in determining the amount of a civil money penalty	Expands the factors considered in determining the amount of a civil money penalty, and adds reference to the imposition of penalties on business associates.	Expands the factors considered in determining the amount of a civil money penalty, and adds reference to the imposition of penalties on business associates.	No Reputational harm to individuals is one of the factors OCR will consider in assessing penalties. Reputational harm is a fact-specific inquiry and it will not be limited to disclosures of sensitive information, such as behavioral health or infectious disease status. Adverse effect on employment or personal relationships and other factors will be considered.
§ 160.410 Affirmative defenses	Revises affirmative defenses consistent with HITECH's tiered penalty scheme and also references business associate liability.	Revises affirmative defenses consistent with HITECH's tiered penalty scheme and also references business associate liability.	No
§ 160.412 Waiver	Updates regulatory references (technical revision)	Updates regulatory references.	No This is a technical revision only.
§ 160.418 Penalty not exclusive	Updates statutory references (technical revision)	Updates statutory references.	No This is a technical revision only.
§ 160.420 Notice of Proposed Determination	Adds requirement the Secretary identify the applicable violation category in §160.404 upon which the proposed penalty amount is based, in addition to the proposed penalty amount, in the notice of proposed determination.	Adds requirement the Secretary identify the applicable violation category in §160.404 upon which the proposed penalty amount is based, in addition to the proposed penalty amount, in the notice of proposed determination.	No
Part 164 – Security and Privacy			
§ 164.102 Statutory basis	Updates to reference HITECH	Updates to reference HITECH	No
§ 164.103 Definitions	No HITECH updates	No updates	No
§ 164.104 Applicability	Adds reference to business associates	Adds reference to business associates	No
§ 164.105 Organizational requirements	Updates business associate-related references for covered components of hybrid entities. Revises regulatory references to include breach notification requirements. Proposes the inclusion of business associate functions within the covered component of a hybrid entity.	Updates business associate-related references for covered components of hybrid entities. Revises regulatory references to include breach notification requirements. Requires the inclusion of business associate functions within the covered component of a hybrid entity.	No OCR was concerned that business associate functions of a hybrid entity could avoid direct liability and compliance obligations under HITECH if those functions were excluded from the covered component/s of a hybrid entity.

§ 164.106 Relationship to other parts	References new, business associate compliance obligations (with Parts 160 and 162)	References new, business associate compliance obligations (with Parts 160 and 162)	No
§ 164.302 Applicability	References business associates' obligation to comply with HIPAA security standards	References business associates' obligation to comply with HIPAA security standards	No
§ 164.304 Definitions	Updates definitions of "Administrative safeguards" and "physical safeguards" to include reference to business associates	Updates definitions of "Administrative safeguards" and "physical safeguards" to include reference to business associates	No
§ 164.306 Security standards: General rules	Updated to impose security standards compliance obligations on business associates	Updated to impose security standards compliance obligations on business associates	No
§ 164.308 Administrative Safeguards	Updated to impose administrative safeguards compliance obligations on business associates. Confirms that business associates – and not covered entities – are responsible for business associate subcontractor compliance.	Updated to impose administrative safeguards compliance obligations on business associates. Confirms that business associates – and not covered entities – are responsible for business associate subcontractor compliance.	No In response to comments, OCR confirmed that business associates are responsible for entering into written business associate agreements with their own subcontractors.
§ 164.310 Physical safeguards	Adds reference to business associate compliance obligations	Adds reference to business associate compliance obligations	No
§ 164.312 Technical safeguards	Adds reference to business associate compliance obligations	Adds reference to business associate compliance obligations	No
§ 164.314 Organizational requirements	Updates business associate contract requirements. Requires business associates to agree to comply with Security Standards, to report breaches of unsecured PHI and to impose the same requirements on business associate subcontractors.	Updates business associate contract requirements. Requires business associates to agree to comply with Security Standards, to report breaches of unsecured PHI and to impose the same requirements on business associate subcontractors.	No OCR's expectation is that business associates and subcontractors should already have security measures in place consistent with the Security Rule or that only require minor updates to comply with HITECH requirements.
§164.316 Policies procedures and documentation requirements	Requires business associates to implement and update security policies and procedures	Requires business associates to implement and update security policies and procedures	No
§164.400 Application Period	Shall apply for breaches occurring on or after September 23, 2009.	Shall apply for breaches occurring on or after September 23, 2009.	No

§164.402 Definitions	Defines breach and provides exclusions to instances that a breach would have occurred. Provides a "harm standard" to define what could be considered a reportable breach.	Modifies the definition of "breach" and revises the risk assessment by eliminating the harm standard previously proposed. Creates an objective, four-factor test for determining whether or not PHI has been compromised and if breach notification is necessary.	Yes The revised definition of "breach," creates a presumption that an impermissible use or disclosure of PHI is a reportable breach, unless the covered entity can demonstrate a low probability that PHI has been compromised by considering at least: 1. The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification; 2. The unauthorized person who used PHI or to whom disclosure was made; 3. Whether the PHI was actually acquired or viewed; and 4. The extent to which the risk to the PHI has been mitigated.
§164.404(a) Discovery of a breach	Breaches will be treated as discovered by the covered entity on the first day that the entity becomes aware of the breach or on the first day that a covered entity should have gained knowledge of the breach through exercising due diligence.	Breaches will be treated as discovered by the covered entity on the first day that the entity becomes aware of the breach or on the first day that a covered entity should have gained knowledge of the breach through exercising due diligence.	No OCR maintained the rule without modification and rejected comments that a breach should only be treated as "discovered" when management is notified of the breach because the HITECH Act itself treats a breach as discovered when "any person, other than the individual committing the breach" who is an employee, officer, or other agent of the entity is aware of the breach.
§164.404(b) Time period of notification	The covered entity must provide notice to all persons affected by the breach within 60 calendar days after discovery of the breach.	The covered entity must provide notice to all persons affected by the breach within 60 calendar days after discovery of the breach.	No OCR reiterates that the 60-day time period for notification begins when the incident is first known, not when the investigation is complete. Additionally, OCR confirms that 60 days is the outer limit for notification. Covered entities are expected to make notifications as soon as reasonably possible. In some cases, it may be an unreasonable delay, and a violation of the regulations, to wait until the 60th day.
§164.404(c) Content of notification	The content of the notification shall include: A) a brief description of the event; B) A description of the types of unsecured PHI involved; C) Steps individuals should take to protect themselves; D) A brief description of steps being taken by the covered entity; E) Contact information for affected individuals to learn more. The notification must be produced in plain language.	The content of the notification shall include: A) a brief description of the event; B) A description of the types of unsecured PHI involved; C) Steps individuals should take to protect themselves; D) A brief description of steps being taken by the covered entity; E) Contact information for affected individuals to learn more. The notification must be produced in plain language.	No OCR believes that the notice content requirements proposed originally provide flexibility to covered entities to tailor their breach notifications to the circumstances while still providing affected individuals with information needed to protect themselves. Further, the content requirements permit disclosure without the risk of creating a road map for third parties for future violations (such as revealing a vulnerability in the covered entity's security infrastructure.

§164.404(d) Methods of notification	The methods by which a covered entity may notify affected individuals are: 1) Written notice either by first-class mail, electronic mail if agreed to by the individual; 2) In cases in which insufficient contact information exists, a "substitute method" of notice can be used, including telephone notice, posting on the entity's home page or conspicuous notice in major print or broadcast media. A toll free telephone number must also be provided.	The methods by which a covered entity may notify affected individuals are: 1) Written notice either by first-class mail, electronic mail if agreed to by the individual; 2) In cases in which insufficient contact information exists, a "substitute method" of notice can be used, including telephone notice, posting on the entity's home page or conspicuous notice in major print or broadcast media. A toll free telephone number must also be provided.	No In its comments, OCR reiterated that a covered entity ultimately maintains the obligation to notify affected individuals of a breach, even if the breach occurred under the business associate and even if the responsibility to notify has been delegated to a business associate. In cases of a breach involving multiple entities, for example from a central Health Information Organization (HIO), it may be necessary for the HIO to notify all potentially affected individuals.
§164.406 Prominent media notification	For breaches involving more than 500 individuals of one State or jurisdiction, the covered entity shall notify prominent media outlets within 60 calendar days.	For breaches involving more than 500 individuals of one State or jurisdiction, the covered entity shall notify prominent media outlets within 60 calendar days.	Yes The change removes a specific reference to American Samoa and the Northern Mariana islands in light of separate revisions to the definition of "state."
§164.408 Notification of Secretary	For breaches affecting more than 500 individuals, the covered entity must immediately notify the Secretary. For breaches affecting fewer than 500 individuals, the covered entity must do so within 60 days of the end of the calendar year in which the breach occurred.	For breaches affecting more than 500 individuals, the covered entity must immediately notify the Secretary. For breaches affecting fewer than 500 individuals, the covered entity must do so within 60 days of the end of the calendar year in which the breach was discovered by the entity.	Yes OCR makes a small but significant change by replacing "discovered" with "occurred." Entities cannot be punished for failure to notify the Secretary within 60 days of calendar year end if they were unaware of the breach during the previous calendar year. Additionally, OCR is considering a less burdensome submission system for smaller breaches and eliminating the requirement that each breach be submitted individually.
§164.410 Business Associate Provisions	Provides similar regulations for any business associate involved in a breach except that it must notify the covered entity not the affected individuals. Additionally, the business associate must provide the covered entity with the identity of each individual whose unsecured protected health information has or could reasonably be assumed to have been affected by the breach. Once the covered	Provides similar regulations for any business associate involved in a breach except that it must notify the covered entity not the affected individuals. Additionally, the business associate must provide the covered entity with the identity of each individual whose unsecured protected health information has or could reasonably be assumed to have been affected by the breach. Once the covered	Yes This section includes technical changes that do not affect the meaning of the rule. In commentary, OCR encourages covered entities and business associates to discuss and define in their business associate agreements the requirements regarding how, when, and to whom a business associate should provide notification in order to expedite notification of affected individuals if necessary.

	entity has notice of the breach, it is up to the covered entity and business associate to decide which is in the best position to notify the individuals affected.	entity has notice of the breach, it is up to the covered entity and business associate to decide which is in the best position to notify the individuals affected.	
§164.412 Law Enforcement Delay	If law enforcement determines that breach notification will inhibit investigation, the covered entity may delay notification for up to thirty days following law enforcement's request to delay.	If law enforcement determines that breach notification will inhibit investigation, the covered entity may delay notification for up to thirty days following law enforcement's request to delay.	No
164.414. Administrative Requirements and Burden of Proof	Requires a covered entity to comply with administrative requirements (updated policies and procedures, training, sanctions policy and documentation) with respect to breach notification. Covered entities and business associates have the burden of proof in demonstrating that all required breach notifications were made.	Requires a covered entity to comply with administrative requirements (updated policies and procedures, training, sanctions policy and documentation) with respect to breach notification. Covered entities and business associates have the burden of proof in demonstrating that all required breach notifications were made.	No
§164.500 Applicability	Makes certain privacy rule provisions applicable to business associates	Makes certain privacy rule provisions applicable to business associates	No
§164.501 Definitions	Updates Health Care Operations definition with reference to Patient Safety Activities (as defined in 42 CFR 3.20) as a permissible health care operation. Updates Marketing definition and lists specific HITECH exceptions to the marketing definition.	Updates Health Care Operations definition with reference to Patient Safety Activities (as defined in 42 CFR 3.20) as a permissible health care operation. Updates Marketing definition and lists specific HITECH exceptions to the marketing definition.	Yes The final rule significantly modifies the proposed rule by requiring authorization for all treatment and health care operations communications where the covered entity receives financial remuneration for making the communication from the third party whose product or service is being marketed.
§ 164.502 Uses and Disclosures of protected health information: general rules	Adds a new section of required and permitted business associate uses and disclosures of PHI. Specifies that a covered entity is not required to obtain satisfactory assurances from a business associate	Adds a new section of required and permitted business associate uses and disclosures of PHI. Specifies that a covered entity is not required to obtain satisfactory assurances from a business associate	No OCR confirms that business associates are directly liable for violations of applicable provisions of the Privacy Rule, for failing to disclose PHI to the Secretary in an investigation, for failing to provide PHI in electronic form when requested by an individual and for failing to enter into subcontracts with subcontractors that use

	subcontractor, and that a business associate is responsible for obtaining such assurances. Limits the protection of PHI of deceased individuals to a period of 50 years following the individual's death.	subcontractor, and that a business associate is responsible for obtaining such assurances. Limits the protection of PHI of deceased individuals to a period of 50 years following the individual's death.	and disclose PHI on their behalf, for failure to provide an accounting and failure to abide by the Security Rule.
§ 164.504 Uses and disclosures, organizational requirements	Adds business associate subcontractor requirements. Eliminates the requirement for a covered entity to report business associate violations to the Secretary if termination of the business associate agreement is not feasible. Creates business associate obligation to terminate subcontracts for covered entity violations. Requires business associates to comply with the HIPAA Security Standards. Requires business associates to report breaches of unsecured PHI. Requires business associates to comply with any covered entity responsibilities delegated to the business associate under the business associate agreement. Requires business associates to impose business associate regulatory and contractual obligations on subcontractors.	Adds business associate subcontractor requirements. Eliminates the requirement for a covered entity to report business associate violations to the Secretary if termination of the business associate agreement is not feasible. Creates business associate obligation to terminate subcontracts for covered entity violations. Requires business associates to comply with the HIPAA Security Standards. Requires business associates to report breaches of unsecured PHI. Requires business associates to comply with any covered entity responsibilities delegated to the business associate under the business associate agreement. Requires business associates to impose business associate regulatory and contractual obligations on subcontractors.	No This section will require business associate agreement updates to eliminate certain notifications to the Secretary. OCR also clarifies that only certain provisions of the Privacy Rule apply to business associates.
§ 164.506 Uses and disclosures to carry out treatment, payment and health care operations	Allow covered entities to disclose PHI to other participants in an organized health care arrangement – not just other covered entities.	Allow covered entities to disclose PHI to other participants in an organized health care arrangement – not just other covered entities.	No
§164.508 Uses and disclosures for which an authorization is required	Updated to reference new "marketing" definition. Requires an authorization for any disclosure of PHI for marketing that involves direct or indirect remuneration. Exceptions	Updated reference to new "marketing" definition. Requires an authorization for any disclosure of PHI for marketing that involves financial remuneration. Moved general prohibition	Yes The final rule significantly modifies the proposed rule by requiring authorization for ALL subsidized treatment and health care operations communications when the covered entity receives financial remuneration from the third party whose

	include: Public health purposes, research purposes, treatment and payment purposes, the sale, transfer or merger of a covered entity and associated due diligence; disclosures to or by business associates if remuneration is limited to compensation for the business associate's services, to an individual, as required by law and for costs associated with transmitting PHI as permitted or required by HIPAA or other applicable law. Permits authorizations for a research study to be combined with another authorization for the same research study, with an authorization for the creation of a research database or repository, or with a consent to participate in research. Authorizations for multiple research uses must specify activities that are conditioned on the authorization and provide an opportunity for individuals to opt out of unconditioned activities.	on sale of PHI by a covered entity or business associate to § 164.502(a)(5)(ii) and created a definition of "sale of protected health information" in that section. Added reference to clarify that other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of PHI which is a sale of PHI, and such authorization must state that the disclosure will result in remuneration to the covered entity. Permits authorizations for a research study to be combined with another authorization for the same research study, with an authorization for the creation of a research database or repository, or with a consent to participate in research. Authorizations for multiple research uses must specify activities that are conditioned on the authorization and provide an opportunity for individuals to opt out of unconditioned activities.	products or services are being marketed.
§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object	Permits a covered entity to disclose PHI to family members or other persons who were involved in the care or payment for health care of a deceased individual prior to his or her death, unless doing so is inconsistent with the prior, express wishes of the deceased.	Permits a covered entity to disclose PHI to family members or other persons who were involved in the care or payment for health care of a deceased individual prior to his or her death, unless doing so is inconsistent with the prior, express wishes of the deceased.	No OCR declined to include language in the final rule placing the burden of proof on the requestor to demonstrate they were involved in the deceased individual's care.
§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required	Permits providers who are not members of an employer's workforce but who provide health care to an individual at the request of the individual's employer	Permits providers who are not members of an employer's workforce but who provide health care to an individual at the request of the individual's employer	No

	to disclose the individual's PHI to the employer. Permits covered entities to disclose student immunization information to schools. Permits the Department of Homeland Security to disclose PHI to the Department of Veterans Affairs to support a DVA determination of eligibility for benefits.	to disclose the individual's PHI to the employer. Permits covered entities to disclose student immunization information to schools. Permits the Department of Homeland Security to disclose PHI to the Department of Veterans Affairs to support a DVA determination of eligibility for benefits.	
§ 164.514 Other requirements relating to uses and disclosures of protected health information	Requires a covered entity to include a clear and conspicuous opportunity to opt out of fundraising communications. Prohibits a covered entity from conditioning treatment or payment on the individual's acceptance of fundraising materials. The marketing exception for health-related communications only applies if i) the covered entity has updated its Notice of Privacy Practices regarding remunerated communications; ii) the communication informs the individual that it is a remunerated communication and that the individual has a right to opt out of such communications.	Requires a covered entity to include a clear and conspicuous opportunity to opt out of fundraising communications and permits a covered entity to provide an individual who has opted out of receiving fundraising communications with a method to opt back in. Permits a covered entity to use or disclose to a business associate or to an institutionally related foundation certain PHI for the purpose of raising funds for its own benefit, including: (i) demographic information related to an individual, including name, address, other contact information, age, gender and date of birth, (ii) dates of health care service provided to an individual, (iii) department of service information, (iv) treating physician, (v) outcome information, and (vi) health insurance status. Prohibits a covered entity from conditioning treatment or payment on the individual's acceptance of fundraising materials. Requires health plans receiving PHI for the purpose of underwriting to only use or disclose PHI as required by law, subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic	Yes The final rule significantly expands the types of PHI that may be used for fundraising purposes.

		information included in the PHI.	
§ 164.520 Notice of privacy practices for protected health information	If the covered entity plans to send health-related communications for remuneration, the notice must make clear that the individual has a right to opt out of such communications.	(1) Notice of Privacy Practices must include a description of the types of uses and disclosures that require authorization; (2) If covered entity engages in listed activities, its notice must contain separate statements for the following: (a) the covered entity may contact the individual to raise funds for the covered entity and the individual can opt out of such communications, and (b) if covered entity that is a health plan intends to use or disclose PHI for underwriting, a statement that the covered entity is prohibited from using or disclosing PHI that is genetic information; (3) Notice must include a statement that covered entity is required to notify affected individuals following a breach of unsecured PHI; (4) Changes in how a health plan gives notice of material changes in notice.	Yes OCR has eliminated the requirement for notice of subsidized health-related communications because other revisions to the rule prohibit these communications without authorization. OCR clarifies that while the final rule requires Notice updates, providers are NOT required to prepare and redistribute paper notices. Rather, they must conspicuously post the revised notice and have copies available upon request at the delivery site. Health plans must post Notice revisions on their websites and provide hard copy Notices to members in the next annual mailing.
§164.522 Right to request privacy protection for protected health information.	A covered entity must agree to an individual's requested restriction on disclosures of PHI to a health plan related to health care for which the individual has paid out of pocket.	A covered entity must agree to an individual's requested restriction on disclosures of PHI to a health plan related to health care for which the individual has paid out of pocket.	No
§ 164.524 Access to PHI	If a covered entity maintains a designated record set in electronic form, it must provide access to an individual in electronic form if the individual so requests. Permits an individual to direct, in writing, a covered entity to transmit a copy of PHI to a third party designated by the	If a covered entity maintains a designated record set in electronic form, it must provide access to an individual in electronic form if the individual so requests. Permits an individual to direct, in writing, a covered entity to transmit a copy of PHI to a third party designated by the	No

	individual. Permits the covered entity to recoup reasonable costs associated with the electronic transfer of PHI.	individual. Permits the covered entity to recoup reasonable costs associated with the electronic transfer of PHI.	
§164.532 Transition provisions	Includes references to business associate compliance obligations.	Includes references to business associate compliance obligations.	No Final rule updates the dates included in the proposed rule, but no change in the timeline.