Update to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules[1]

Released by HHS January 25, 2013

This article provides an overview of the January 25, 2013 Final Rule update to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")[2] which was published by the Department of Health and Human Services ("HHS"). The Final Rule provides modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act ("HITECH")[3] and the Genetic Information Nondiscrimination Act ("GINA").[4] This article will provide a brief overview of HIPAA to provide a baseline and then review the major provisions of the Final Rule.

Overview

HIPAA provides regulations for the privacy and security of Protected Health Information ("PHI") which is individually identifying information to include:

> [D]emographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual;

---

[1] Analysis in this article is for informational and reference purposes only. If you have a matter requiring legal assistance, it is recommended you consult with a licensed attorney. The Final Rule is available on the Department of Health and Human Services website: http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

[2] HIPAA, Pub. L. 104-191, 110 Stat. 1936, included "Administrative Simplification" provisions under which privacy and security standards were issued.

[3] Enacted under Title XIII of the American Recovery and Reinvestment Act (Pub.L. 111-5, 123 Stat. 227).

[4] Pub. L. 110-233, 122 Stat. 881.

> or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[5]

The HIPAA rules apply to Covered Entities, which are health plans, health care clearinghouses or a health care provider who transmits any health information in electronic form.[6] A HIPAA Business Associate is a person or entity who provides a function or activity for a Covered Entity involving the use or disclosure of individually identifiable health information and is not part of the workforce of the Covered Entity.[7]

The HIPAA Privacy Rule requires a Covered Entity to disclose PHI in only two situations: 1) to HHS for investigations; and 2) to the patient upon their request unless an exception applies.[8] A Covered Entity is permitted to disclose PHI for the treatment[9], payment[10] or use in health care operations[11].[12] The Security Rule requires a Covered Entity to:

---

[5] 45 CFR § 160.103.

[6] 45 CFR § 160.103.

[7] 45 CFR § 160.103.

[8] 45 CFR § 164.502(a)(2).

[9] Treatment is the provision, coordination, or management of health care and related services for an individual, including consultation between providers and referral of an individual to another provider for health care. 45 CFR § 164.501.

[10] Payment includes activities of a health care provider to obtain payment or to receive reimbursement for the provision of health care to an individual. 45 CFR § 164.501.

[11] Health care operations includes functions such as: (a) quality assessment and improvement; (b) competency assessment,, including performance evaluation, credentialing, and accreditation; (c) medical reviews, audits, or legal services; (d) specified insurance functions; and (e) business planning, management, and general administration. 45 CFR § 164.501.

[12] 45 CFR § 164.502(a)(1).

> (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the Covered Entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required…. (4) Ensure compliance with this [rule] by its workforce.[13]

HHS issued Interim Final Rule on August 24, 2009, that implemented the HITECH breach notification requirements. This required a Covered Entity to provide notification to affected individuals and HHS if their PHI was breached unless an exception applied.[14] To determine whether notice to the individual is required, a Covered Entity must determine whether the use or disclosure violated the HIPAA Privacy Rule and if significant risk of financial, reputation or other harm may befall the individual.[15] Additionally, for breaches of more than five hundred (500) individuals, a press release should be provided to local media outlets.[16] A Business Associate must give notice to a Covered Entity if any of the PHI they are responsible for is compromised.[17]

Violations of the HIPAA Privacy and Security Rules may result in civil and criminal penalties. The Civil Monetary Penalties ("CMP") provisions apply to Covered Entities and HITECH extends those provisions to include Business Associates.[18] HHS uses a tiered

---

[13] 45 CFR §164.306.

[14] 75 FR 19006.

[15] 75 FR 19006.

[16] 75 FR 19006.

[17] 45 CFR § 164.410.

[18] 42 USC § 1320d-5; 45 CFR § 160.404.

evaluation in assessing penalties based on the entity's actions[19] and in some instances, a person may be held criminally liable and receive a prison sentence, duration of which is ultimately based on the nature of the breach.[20] GINA prohibits using genetic information for employment or health insurance discrimination.[21]

Final Rule – January 25, 2013

The Final Rule became effective on March 26, 2013 and requires all Covered Entities and Business Associates to comply with the new provisions by September 23, 2013. It is composed of four sections and will be reviewed in that particular order. For reference purposes, where the Final Rule is discussed, the page number is footnoted so that the reader may easily find the information for further clarification or detail.

1. Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, and certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010.

A. Expansion of the Definition of "Business Associate"

One of the major changes the Final Rule makes is an expansion of the definition of a Business Associate. First, patient safety activities were added to the list of functions and activities a person or organization may perform on behalf of a Covered Entity that gives rise to a Business Associate relationship.[22] Second, a Health Information Organization, E-prescribing

---

[19] 42 USC § 1320d-5; 45 CFR § 160.404.

[20] 42 USC § 1320d-6.

[21] Pub. L. 110-233, 122 Stat. 881.

[22] 5570.

Gateway, or other persons that provide data transmission services with respect to PHI to a Covered Entity and requires routine access to that data, would be included in the definition of a Business Associate.[23] This would also include a person who offers a personal health record on behalf of a Covered Entity.[24] However, a person or entity that is merely a transmission service or conduit (e.g. postal carrier or internet service provider) would not be included in this modified definition.[25] Third, a Subcontractor, which is "a person to whom a Business Associate has delegated a function, activity or service the Business Associate has agreed to perform for a Covered Entity or Business Associate" who creates, receives, maintains or transmits PHI on behalf of the Business Associate, to be included in the expanded definition.[26] Therefore, a Business Associate and their Subcontractor are required to enter into a Business Associate Agreement ("BAA") when HIPAA protected information is involved. The Final Rule clarified that a Covered Entity does not have to enter into a Business Associate Agreement with a Business Associate's Subcontractor[27] but it would be the responsibility of the Business Associate to obtain satisfactory assurances that the Subcontractor would not improperly disclose PHI.[28] However, the Covered Entity does have a responsibility to include in the Business Associate Agreement with the Business Associate that the Business Associate must ensure that all Subcontractors will abide by the same restrictions and conditions that apply to the Business

---

[23] 5571.

[24] 5571.

[25] 5571.

[26] 5572-73.

[27] 5590.

[28] 5599

Associate.[29] That being said, a BAA between a Subcontractor and a Business Associate may not permit the Subcontractor to use or disclose PHI that would be impermissible for the BA.[30] However, the Final Rule modified the Business Associate Agreement requirements in that a Business Associate and a Subcontractor must enter into a Business Associate Contract that includes all the terms and conditions mandated by the HIPAA Privacy and Security Rules. Furthermore, a Business Associate must ensure any Subcontractor that enters into a contract to protect electronic PHI and those arrangements between a Covered Entity and Business Associate would apply in the same manner as arrangements between the Business Associate and the Subcontractor.[31] The Final Rule also establishes that a person can become a Business Associate by definition of their activities and relationships with the Covered Entity or Business Associate, not requiring a need to formally enter into a Business Associate Agreement.[32] Thus, liability for any improper use or disclosure attaches immediately when a person creates, receives, maintains or transmits PHI.[33]

The Final Rule grants a one year transition period that enables entities to modify their Business Associate Agreements to comply with this new rule.[34] This applies to evergreen agreements that automatically renew and new Business Associate Agreements that have recently been negotiated in good faith.[35]

---

[29] 5601.

[30] 5601.

[31] 5590.

[32] 5598.

[33] 5598.

[34] 5603.

[35] 5603.

B. Marketing Communications

The Final Rule adopts a broad rule that requires "authorization for all treatment and health care operations communications where the Covered Entity receives financial remuneration for making the communication from a third party whose product or service is being marketed."[36] Financial remuneration, for the purposes of marketing, means "direct or indirect payment from or on behalf of a third party whose product or services is being described."[37] This definition does not include any non-financial benefits and the financial remuneration provided to the Covered Entity by the third party must be specifically for making the communication which encourages a person to utilize or purchase the third party's product or service.[38] The Final Rule specifically states that if the "financial remuneration received by the Covered Entity is for any purpose other than for marketing the communication, then the marketing provision does not apply."[39] Since the Final Rule concludes that subsidized treatment communications are marketing communications, a Covered Entity's notice of privacy practices no longer requires a statement informing persons that the Covered Entity may send to an individual notice of alterative treatments or other health related products/services in which financial remuneration is provided to the Covered Entity for sending the communication nor the individual has a right to opt out of receiving these types of communications.[40] The Final Rule clarified that whereas a businesses associate, including a Subcontractor, receives financial remuneration from a third

---

[36] 5595.

[37] 5593.

[38] 5596.

[39] 5596.

[40] 5595.

party for communicating a product or service to an individual, that communication also requires the individual's prior authorization.[41] Although the Final Rule is broad, it does identify exceptions. No authorization is required "where a Covered Entity receives financial remuneration from a third party to make a treatment or health care operations communication (or other marketing communication), if the communication is made face-to-face by a Covered Entity to an individual or consists of a promotion gift of nominal value."[42] However, this exception does not apply to communications over the phone, email or general mail.[43] Another exception is communications promoting general health but not abdicating a specific product or service (i.e. annual mammograms).[44] Also, communications about government or government sponsored programs are excluded.[45] Additionally, communications describing a Covered Entity's health related products and services, reminders to refill prescriptions for drugs or biologics taken by the individual so long as the financial remuneration received by the Covered Entity is reasonably related to the cost of making the communications and marketing for non-treatment functions.[46]

C. Right to Request a Restriction of Uses and Disclosures

The Final Rule requires a Covered Entity to take steps to protect PHI, when restriction is requested by the individual, from subsequent disclosures to a health plan for payment or operations unless otherwise required by law.[47] If required by law, the disclosure should be made

---

[41] 5595.

[42] 5596.

[43] 5596.

[44] 5597.

[45] 5597.

[46] 5593.

[47] 5628.

by the Covered Entity even if the individual protests.[48] Also, if an individual refuses to permit a Covered Entity to submit a claim to a health plan, including Medicare, the Covered Entity may accept out of pocket payment from the individual and not submit a claim.[49]

D. Patient Access to PHI in Electronic Format

The Final Rule provides an individual the right to request an electronic copy of PHI and the Covered Entity must provide access to the information in an electronic form and format requested by the individual.[50] If the Covered Entity cannot provide the PHI in the requested format, it is sufficient to provide it in a readable electronic form and format so long as the parties agree.[51] The Covered Entity may charge a fee for costs associated with labor and supplies for creating the copy.[52] A Covered Entity may seek a thirty day extension in providing access to the data but only after providing a written explanation as to why an extension is needed.[53]

E. Prohibition on the Sale of PHI

The sale of PHI means "a disclosure of protected health information by a Covered Entity or Business Associate, if applicable, where the Covered Entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information."[54] Excluded in this definition are payments to a Covered Entity for certain types of grants or arrangements to perform programs or

---

[48] 5628.

[49] 5628.

[50] 5681.

[51] 5681.

[52] 5681.

[53] 5681.

[54] 5606.

activities (e.g. research studies) because any access to PHI by the payer is a byproduct of the service.[55]

F. Protection for Decedent Information

A decedent's PHI is to be protected for fifty (50) years as it is difficult to obtain proper authorization for release of information after that extensive period of time.[56] It was noted that fifty years was not a record retention requirement.[57] Also, covered entities may disclose a decedent's PHI earlier than fifty years to family members and others who were directly involved in the care and/or payment of the decedent's care prior to his or her death, unless that contravenes prior expressed wishes by the decedent and the Covered Entity was aware of those wishes.[58]

G. Fundraising

Although the Privacy Rule already permits covered entities to use or disclose demographic information for fundraising communications, the Final Rule clarifies that demographic information pertaining to an individual includes name, address, other contact information, age, gender and date of birth.[59] Additionally, a Covered Entity may disclose health insurance status, dates of health care provided, department of service, treating physician information and outcome information for fundraising purposes.[60]

H. Notice of Privacy Practices ("NPP") for Protected Health Information

---

[55] 5606.

[56] 5614.

[57] 5614.

[58] 5615.

[59] 5621.

[60] 5622.

The NPP must contain a statement with regards to authorizations for use and disclosure of: psychotherapy notes (where appropriate); PHI for marketing purposes; sale of PHI; and a statement that other disclosures not described in the NPP will only be made with the authorization of the individual.[61] Also, the NPP must state that an individual has the right to opt out of fundraising communications if the entity intends to contact individuals for fund raising activities.[62] The NPP must inform individuals of their right, if they pay out of pocket in full for health care, to restrict certain PHI disclosures to a health plan.[63] Finally, the NPP must have a statement of the right of an individual to be notified following a breach of unsecured PHI.[64]

I. Additional Definitions and Provisions

- Minimum Necessary Standard. Business Associates must use the minimum necessary standard when using, requesting or disclosing PHI to or from another Covered Entity or Business Associate.[65] How the standard will be applied will depend on the circumstances.[66]
- Future Research. The Final Rule does not modify or change the authorization requirements for research but no longer requires the authorization to cite the specific study.[67]

---

[61] 5624.

[62] 5624.

[63] 5624.

[64] 5624.

[65] 5599.

[66] 5599.

[67] 5612.

- Disclosures of Student Immunization to Schools. Changes the requirement to permit a Covered Entity to disclose proof of immunization to schools, where that proof is required by law, but the Covered Entity must document permission from the parent or guardian of the student.[68]
- Electronic Media. Modified the definition to include "transmission media" which includes "the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission."[69]

2. Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.

The Final Rule retained the penalty structure that was revised by the Interim Final Rule regarding the CMP provisions that apply to HIPAA violations.[70] The violation categories and potential penalties are:

Violation Category	**Each Violation**	**Calendar Year Cap**
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause[71]	$1,000 - $50,000	$1,500,000

[68] 5617.

[69] 5688.

[70] 5583.

Willful Neglect[72] - Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect - Not Correct	$50,000	$1,500,000

Therefore, it is necessary to be mindful of the dangers associated with noncompliance and take proactive action to mitigate any risks.

3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's ''harm'' threshold with a more objective standard and supplants an interim final rule published on August 24, 2009.

Breach is defined as the "unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."[73] There are three exceptions in that breach:

1) excludes any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a Covered Entity or Business Associate, if such acquisition, access, or use was made in good faith and within the scope of employment or other relationship;
2) excludes inadvertent disclosures of protected health information from a person who is authorized to access protected health information at a Covered Entity or Business Associate to another person authorized to access protected health

[71] Reasonable cause means "circumstances that would make it unreasonable for the Covered Entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated." 45 CFR § 160.401.

[72] Willful neglect means "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." 45 CFR § 160.401.

[73] 42 USC § 17921.

information at the same Covered Entity, Business Associate, or organized health care arrangement in which the Covered Entity participates; and

3) does not include disclosures of protected health information where a Covered Entity or a Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.[74]

Because the Covered Entity or Business Associate has burden of proof to prove that a breach falls within these three exception, they must document why and how the breach falls under one of these exceptions.[75]

The Final Rule amended the breach definition to clarify that "an impermissible use or disclosure of protected health information is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised."[76] Now, instead of the Covered Entity or Business Associate demonstrating that there is no significant risk of harm to the individual whose PHI was breached, the Covered Entity or Business Associate must demonstrate through a risk assessment, that there is a low probability that PHI had been compromised.[77] In performing the risk assessment, the following four factors should be utilized:

(1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the protected health information or to whom the disclosure was

[74] 5640.

[75] 5640.

[76] 5641.

[77] 5641.

> made; (3) whether the protected health information was actually acquired or viewed; and (4) the extent to which the risk to the protected health information has been mitigated.[78]

The Final Rule amended the unsecured PHI definition by changing "unauthorized individuals" with "unauthorized persons" so that "unsecured protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons though the use of technology or methodology specified by the Secretary in guidance."[79]

The Final Rule adopted the Interim Final Rule's provisions relating to notification to individuals whose PHI was breached. The Final Rule clarified that the breach of unsecured PHI is to be treated as discovered on the first day the breach is known or "by exercising reasonable diligence would have been known to the Covered Entity."[80] It is important to note that the discovery date does not change if an employee is aware of the breach but does not inform management. A Covered Entity must notify individuals of a breach without unreasonable delay and no later than sixty calendar days from the discovery of the breach.[81] The Final Rule clarifies that the time period begins not when the investigation is completed by when the incident is discovered.[82] The breach notification, which should be in plain language, must include:

> (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (2) a description of the types of unsecured protected health information that were involved in the breach (such as

[78] 5642.

[79] 5647.

[80] 5647.

[81] 5648.

[82] 5648.

> whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (3) any steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the Covered Entity involved is doing to investigate the breach, mitigate the harm to individuals, and to protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a tollfree telephone number, an email address, Web site, or postal address.[83]

Notice should be provided to the individual via first class mail or electronic mail if the person had previously consented, or substitute notice provided if the individual's contact information is out dated.[84] If there is a reason to believe that a breach may result in the imminent misuse of PHI, telephone or other immediate notice should be provided.[85] If the aggrieved individual is a minor or lacks legal capacity, either due to a physical or mental limitation, notice should be provided to the parent or personal representative.[86] If the person is deceased, then notice must be given to either the personal representative or the next of kin.[87] In the event the Covered Entity does not have proper contact information, the substitute notice used must "be reasonably calculated to reach the individuals for whom it is being provided."[88] If the Covered Entity lacks contact information for ten or more individuals, the Covered Entity must provide substitute

[83] 5648.

[84] 5469.

[85] 5649.

[86] 5649.

[87] 5649.

[88] 5649.

notice "through either a conspicuous posting for a period of 90 days on the home page of its Web site or conspicuous notice in major print or broadcast media in geographic areas where the individual affected by the breach likely reside."[89] The Final Rule notes the Covered Entity maintains the ultimate responsibility for providing notice but can delegate the notice to a Business Associate that suffered the breach.[90] For breaches involving five hundred persons or more in one state or jurisdiction, the Covered Entity must provide notice of the breach to prominent media outlets of that state or jurisdiction.[91] In the event that a breach has occurred of more than 500 individuals but they reside in multiple states or jurisdictions, media notification is only required in the area in which at least 500 individuals reside. The Final Rule did amend the definition of "State" so that it now includes American Samoa and the Northern Mariana Islands.[92] The Final Rule reiterated that immediate notice must be provided to HHS for breaches exceeding 500 individuals and all others must be maintained in a log by the Covered Entity and submitted annually.[93] The Final Rule did clarify that notice to HHS for breaches impacting fewer than 500 individuals must be provided no later than sixty days after the calendar year in which the breaches were discovered, not when the breaches occurred.[94] A breach by a Business Associate must be reported to the Covered Entity when it is discovered and no later than sixty days, to include the identity of the individuals' whose information was breached.[95]

---

[89] 5650.

[90] 5650.

[91] 5652.

[92] 5653.

[93] 5653.

[94] 5654.

[95] 5655

4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009.

GINA prohibits an organization from using genetic information in determining health care coverage and for employment consideration. The Final Rule extends GINA's discrimination prohibition to all health plans subject to the HIPAA privacy rule so that PHI that is genetic information cannot be used for underwriting purposes except for long term care policies.[96] Additionally, the Final Rule adopted various changes to GINA that were published by HHS on July 14, 2010 in a notice of public rule making ("NPRM"). The relevant NPRM changes include clarifying the definition of "health information" to specifically include the term "genetic information", which is defined as:

> [A]ny individual, information about: (1) Such individual's genetic tests; (2) the genetic tests of family members of such individual; and (3) the manifestation of a disease or disorder in family members of such individual (i.e., family medical history)…. GINA… includes, with respect to any individual, any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by such individual or family member of such individual.[97]

The NPRM defined Genetic Test to mean to mean ''an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes'' and specifically does "not include an analysis of proteins or metabolites that does not

---

[96] 5659.

[97] 5561.

detect genotypes, mutations, or chromosomal changes, nor does it include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved."[98] Genetic services are "(1) A genetic test; (2) genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) genetic education."[99] The Final Rule also adopted the NPRM's definition of family member to mean "(1) A dependent… of such individual; or (2) any other individual who is a first degree, second-degree, third-degree, or fourth-degree relative of such individual or of a dependent of the individual."[100] The NPRM defined dependent as "an individual who is or may become eligible for coverage under the terms of a group health plan because of a relationship to the plan participant."[101] The Final Rule also adopted the NPRM's definition of "manifestation or manifested" which means "with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved" and "that a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information."[102] The Final Rule also expressly prohibits health plans from using or disclosing genetic information for underwriting purposes and requires a health plan to provide this notice on their NPP.[103]

---

[98] 5662.

[99] 5662.

[100] 5663.

[101] 5663.

[102] 5663.

[103] 5665.

Next Steps

Due to the changes outlined in the Final Rule, Covered Entities and Business Associates should review their policies and procedures to ensure they are compliant with these provisions. Furthermore, organizations should conduct training so their employees understand the impact these changes may have in how they conduct their operations. Also, Covered Entities should review their Business Associate Agreements and amend if necessary; to make sure they are compliant.

1835469.1