

MGMA GOVERNMENT AFFAIRS

MGMA HIPAA Breach Toolkit

MGMA Government Affairs has developed this toolkit to assist practice leaders better understand and implement the Department of Health and Human Services HIPAA Breach requirements.

MGMA
Medical Group Management Association®

INTRODUCTION

Patient information is increasingly at risk of being inappropriately disclosed. This could occur through such events as loss or theft of a paper record or mobile device (laptop, tablet, cell phone) that contains protected health information (PHI), theft of office computers or servers, inappropriate access to PHI by staff or external individuals, or ransomware or other types of hacking attacks. This toolkit is designed to guide practice executives through the process of determining if a reportable breach occurred and the steps to take if the organization determines that a breach did occur.

WHAT IS CONSIDERED PHI

PHI is information held or transmitted by a practice or its business associate, in any form, whether electronic, paper, or verbal that relates to all of the following:

- The individual's past, present, or future physical or mental health or condition;
- The provision of healthcare to the individual; and
- The past, present, or future payment for the provision of healthcare to the individual.

TIP: PHI can include many common patient identifiers, such as, but not limited to, name, address, birth date, and Social Security number. Practices should also be aware that unique distinguishing characteristics of a patient can serve as an identifier and should be safeguarded.

Step One – Determine If a Breach Occurred

BREACH DEFINITION AND EXCEPTIONS

The Department of Health and Human Services (HHS) definition of a breach is “an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.” HHS outlines three exceptions to the definition of “breach:”

1. Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a practice or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
2. The inadvertent disclosure of PHI by a person authorized to access PHI at a practice or business associate to another person authorized to access PHI at the practice or business associate, or “organized health care arrangement” in which the practice participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule; and
3. If the practice or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information.

RENDERING THE PHI UNUSABLE

Practices that render the PHI unusable, even if that PHI is disclosed, should not consider that disclosure a breach. HHS considers PHI unusable when:

1. Electronic PHI has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and such confidential process or key that might enable decryption has itself not been breached.

TIP: To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt.

2. The media (device hard drive, portable electronic storage device such as CD-ROM or flash drive, film or electronic image, or paper) on which the PHI is stored or recorded has been destroyed in one of the following ways: (i) the media has been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. (Note that HHS states that redaction is specifically excluded as a means of data destruction.); (ii) electronic media have been cleared, purged, or destroyed such that the PHI cannot be retrieved.

TIP: PHI may be stored on any device or machine that has a hard drive and/or is networked. These could include medical devices, printers, and copiers. Ensure that no PHI is accessible when disposing of these.

View the [HHS Guidance](#) Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

Step Two – Determine When and What Happened

Once the practice has determined that a security incident has occurred, the organization should take the steps necessary to answer the following questions:

1. To the best knowledge of the staff, when did the breach occur and when did it end?
2. Who brought the breach to the attention of the practice?
3. Is the breach ongoing? If yes, what steps has the practice taken to prevent any further disclosure of PHI?
4. If yes, what steps does the practice need to take to prevent any further disclosure of PHI?
5. Has the breach impacted the ongoing operations of any clinical or administrative systems (i.e., in the case of a ransomware attack)?
6. How many individuals are affected by the breach?

7. What is the nature of the breach?
 - Loss or theft (include the specific PHI repository, device, or devices)
 - Unauthorized access/disclosure by (i) practice employed staff; (ii) practice volunteer staff; (iii) patients; (iv) contracted service individuals (i.e., cleaning staff); (v) non-business associate vendors; (vi) other external individuals; (vii) unknown
 - Improper disposal of PHI (include the specific repository, device, or devices)
 - Hacking/IT Incident (include as much information as known)
8. If applicable, where in the practice did the breach occur?
9. If applicable, what online environment did the breach occur (i.e., patient portal)
10. What type of PHI is involved?
 - Clinical (i.e., medical records)
 - Financial (i.e., claims data)
 - Patient demographic (i.e., address, insurance information)
 - Patient financial (i.e., credit card information, banking information)
 - Patient social security number or Medicare Beneficiary Identifier
 - Other (define)
11. Was encryption used on any impacted devices?
12. In the case of a ransomware attack, has the practice been contacted regarding the payment of a ransom?

Note: If a business associate was involved, many of the above questions will need to be asked of them.

TIPS: Practices are encouraged to document this discovery process as this information may be important should there be any government enforcement action.

Practices may want to retain the services of an information technology/security firm to assist the organization determine when and how the breach occurred. Further, if the breach is ongoing (i.e., PHI is being inappropriately disclosed on the practice website or there has been a ransomware attack), technical assistance may be required to immediately address the breach or attack.

Step Three – Performing a Risk Assessment

Practices should consider an impermissible use or disclosure of PHI to be a breach unless the practice or their business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment. In performing a risk assessment, the practice can take into account:

1. The nature and extent of the PHI involved, including the types of patient identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the 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.

Step Four – Complying with the Breach Notification Requirements

Once the practice has determined that a breach has occurred, or by “reasonable diligence should have known,” notification must be made to the following entities:

1. **Notice to the impacted individual** – Following the discovery of a breach of unsecured PHI, the practice must notify affected individuals. This notice process includes:
 - a. Providing the notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.
 - b. Should the practice have insufficient or out-of-date contact information for 10 or more affected individuals, the practice is required to either post the notice on the home page of its web site for at least 90 days or provide the notice in major print or broadcast media where the affected individuals likely reside. The practice must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. If the practice has insufficient or out-of-date contact information for fewer than 10 individuals, the practice is permitted to provide substitute notice by an alternative form of “written notice, by telephone, or other means.”
 - c. The practice must provide individual notifications “without unreasonable delay” and in no case later than 60 days following the discovery of a breach.

- d. The notification is required to include, to the extent possible: (i) a brief description of the breach; (ii) a description of the types of information that were involved in the breach; (iii) the steps affected individuals should take to protect themselves from potential harm; (iv) a brief description of what the practice is doing to investigate the breach, mitigate the harm, and prevent further breaches; and (v) contact information for the practice (or business associate, if applicable).
2. **Notice to the HHS Secretary** – Practices are required to notify the federal government should they experience a breach of unsecured PHI. Notification is done by visiting the HHS web site and filling out and electronically submitting a breach report form. There are different requirements depending on the number of affected individuals:
 - a. For breaches that affects **500 or more individuals**: practices are required to notify HHS “without unreasonable delay” and in no case later than 60 days following a breach. Here is the link to the [HHS portal](#) to report a breach of 500 or more individuals. For these breaches, HHS will post the incident on its public [Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information](#) website.
 - b. For breaches that affects **fewer than 500 individuals**: practices may notify HHS of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to HHS no later than 60 days after the end of the calendar year in which the breaches are discovered. Here is the link to the [HHS portal](#) to report a breach involving fewer than 500 individuals.
 3. **Notice to the Media** – For breaches involving more than 500 residents of a State or jurisdiction, practices are required to provide notice to prominent media outlets serving the State or jurisdiction. Practices will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Media notifications must be provided “without unreasonable delay” and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

BUSINESS ASSOCIATE NOTIFICATION REQUIREMENTS

If a breach of unsecured PHI occurs at or by a business associate, they must notify the practice following the discovery of the breach “without unreasonable delay” and no later than 60 days from the discovery of the breach. HHS stipulates that, to the extent possible, the business associate should provide the practice with the identification of each individual affected by the breach as well as any other available information required to be provided by the practice in its notification to affected individuals.

In the case of a breach that happens at or is caused by a business associate, while the practice is ultimately responsible for ensuring individuals are notified, practices are permitted to delegate the responsibility of providing individual notices to the business associate.

TIP: Practices and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the practice and which entity has the relationship with the individual.

HHS GUIDANCE ON BUSINESS ASSOCIATES

In a FAQ, HHS addresses the issue of whether a practice is liable for, or required to monitor, the actions of its business associates. HHS stipulates that while practices are required to enter into a business associate agreement with these entities to protect the privacy of PHI, practices are not liable for the actions of the business associate and they are not required to “monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract.” However, if a practice finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate.

TIP: Practices are encouraged to review their current business associate agreements and consider including in the agreement: (i) stipulation that the business associate will contact the practice within 10 days of a breach being discovered; (ii) that the business associate will provide a complete accounting of how the breach occurred and number of affected individuals; and (iii) that the business associate will provide a report outlining the steps they are taking to mitigate the breach and its impact on affected individuals.

Step Five-Documentation

Should a practice believe that the disclosure of unsecured PHI did not constitute a breach, it is required to retain documentation establishing the process undertaken by the organization in making that determination. As part of this documentation requirement demonstrating that notification of the breach was not required, practices should document and retain:

1. A full description of the risk assessment conducted by the practice demonstrating a low probability that the PHI has been compromised by the impermissible use or disclosure; or
2. The application by the practice of any other exceptions to the definition of breach.

In a case where the practice determined that a breach of unsecured PHI did in fact occur and notice was provided to affected individuals, practices should document and retain all information establishing that the required notifications were provided to affected individuals, to HHS, and to local media (as applicable).

TIP: Practices are also required to comply with certain administrative requirements with respect to breach notification. For example, practices must have in place written policies and procedures regarding breach notification, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures. Documentation that the practice has complied with these requirements is highly recommended.

Legal Disclaimer

The information provided in this document does not, and is not intended to, constitute legal advice. Instead, all information in this document is for general informational purposes only. Readers of this document should contact an attorney to obtain advice with respect to any particular legal matter.

A grayscale photograph of a hand holding a pen, poised to write on a document. A semi-transparent teal rectangular overlay covers the middle portion of the image, containing the text. The background is blurred, showing what appears to be a person's face in the upper half.

Visit mgma.com/hipaa for additional MGMA and federal government resources.

