IGC™
Informative Graphics Corporation

Redaction in health information management

AN IGC WHITE PAPER

The health information management (HIM) department in a hospital or the healthcare provider in a practice are stewards of the provider's medical records. A great deal of responsibility lies within this role—which is one reason why the HIM profession emphasizes specific education and credentials for its professionals. HIPAA compliance is not to be taken lightly, and this is especially important during the release of information (ROI) process. Redaction (removal) of protected health information or other data outside of the information determined to be the "minimum necessary" for disclosure is often necessary to ensure compliance.

Though this paper focuses on redaction by healthcare providers, other HIPAA covered entities (such as health plans) and business associates also should be routinely redacting protected health information and have policies in place to determine both when redaction is required and how it should be performed.

Protecting sensitive information during ROI

ROI is the process of responding to external requests for all or parts of a patient's medical record. The requestors can be the patients themselves, providers, health insurance companies, life insurance companies validating medical histories, attorneys for auto insurance companies, workers' compensation carriers and others.

Requests for medical records under the ROI process are often very specific, and the specificity is facilitated by the providers' ROI forms. Such forms may allow the requestor to specify dates of service, and often require the requestor to actively select whether certain protected health information categories are to be included. In some cases, the HIM department may require patient consent, if authorization was not already obtained, to ensure compliance with HIPAA or state medical record privacy laws.

At minimum, special consideration for redaction should be given to the following categories of protected health information:[1] [2]

- Domestic violence
- Genetic information
- Mental health information (Psychotherapy notes cannot be disclosed without explicit authorization.)
- Reproductive health
- HIV/AIDS
- Substance abuse (Federally funded substance-abuse program information cannot be disclosed without explicit authorization.)
- Information resulting from visits paid for out of pocket (This pertains to disclosure to health insurance companies only.)
- Information resulting from a visit paid for in cash, as established in the HITECH Act
- Additional categories may be determined by state laws

HIPAA compliance is gaining increasing attention as the U.S. Department of Health and Human Services' Office for Civil Rights responds to and investigates complaints and breaches. It is broadly known, however, that small breaches—such as disclosing a single individual's protected health information to those who should not see it—occur on a much more frequent basis than the large breaches that are reported in the news.

Using redaction to maintain HIPAA compliance

Prior to the passing of the HITECH Act (part of the American Recovery and Reinvestment Act of 2009), a person requesting a record often determined the extent of the "minimum necessary" information they desired to receive, as HIPAA did not explicitly define the term. Section 13405(b)(2) of the HITECH Act, however, specifies that "the covered entity or business associate disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure."[3] This places even more responsibility for HIPAA compliance on the disclosing party.

HIPAA covered entities and business associates need to be aware of protected health information contained in records and be able to redact (remove) this information as necessary to prevent accidental disclosures. Though an electronic health record (EHR) system often has the capability to include only specified information when responding to a ROI request, any patient's EHR may include unstructured documents such as scanned medical records in TIFF or PDF format predating the EHR, or documents from other systems in the hospital such as emergency department discharge summaries or radiology reports. HIM departments often combine multiple documents into a single PDF for release. Since a medical record for a single patient may run into the thousands of pages, the ability to create and run programmed redaction scripts to redact specific terms (e.g., Social Security numbers or the name of a medication implying a sensitive condition) or term groups (words known to be associated with a specific condition, for example) can save both time and money, while ensuring HIPAA compliance.

Redaction is also required for the de-identification of unstructured documents, which requires either the use of expert determination through statistical analysis or by following the HIPAA Safe Harbor standard. This method requires removing 18 HIPAA-specified identifiers associated not only with the patient, but also with their household members, relatives and employers.[4] With the increasing interaction between pharmaceutical companies, academic researchers and providers, including large providers with their own grant-sponsored research teams, complete de-identification or creation of a "limited data set" of allowed identifiers is often necessary.

Using the Safe Harbor method, de-identification requires removal of the following identifiers:[5]

1. Names
2. Geographic subdivisions smaller than a state, such as address, ZIP code and so on
3. Dates (except for the year)
4. Telephone numbers
5. Email addresses
6. Fax numbers
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate or license numbers
12. Vehicle identifiers
13. Device identifiers such as serial numbers
14. Web URLs
15. IP addresses
16. Biometric identifiers
17. Full-face photographs and comparable images
18. Any other unique identifying number, characteristic or code

Ensuring effective redaction of protected health information

Large-scale de-identification of documents can be performed using server-based redaction systems, which saves time and money when thousands of documents are involved, such as in hospital-based eDiscovery scenarios. Quality assurance processes can be performed subsequently with a user interface to ensure that redaction was effective and complete (OCR success rates affect this ability).

Today, unfortunately, from the most sophisticated hospitals' HIM departments to single-provider offices, redaction is often still performed manually using permanent markers and pens. If electronic redaction occurs, which is currently rare, it is performed through a third-party application that is not integrated with the medical record system.

Hospitals and provider practices may outsource the ROI process, but if redaction is anticipated or required, ROI firms often route such requests back to providers for completion. A few ROI firms will perform redaction as needed, but this is not the norm. Ensuring that ROI firms properly identify requests that require redaction should be part of any oversight by the hospital HIM department, with criteria and associated redaction processes detailed in the ROI outsourcing contract.

Summary

Performing redaction within existing workflows, such as while viewing documents in either an EHR system or a document management and imaging system (which may be integrated into an electronic content management system), is key. Document viewers should include options for redaction to ensure that users can maintain HIPAA compliance while keeping efficiencies high.

[1] The American Recovery and Reinvestment Act of 2009. "HITECH Act." February 13, 2009. www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf

[2] National Committee on Vital Health Statistics. Letter to Secretary Sebellius "Re: Recommendations Regarding Sensitive Health Information." November 10, 2010. www.ncvhs.hhs.gov/101110lt.pdf

[3] The American Recovery and Reinvestment Act of 2009. "HITECH Act."

[4] U.S. Department of Health and Human Services. "Workshop on the HIPAA Privacy Rule's De-Identification Standard." March 10, 2012. www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/deidentificationworkshop2010.html

[5] U.S. Department of Health and Human Services. "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule." November 26, 2012. www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

About IGC

IGC is a recognized leader in viewing, collaboration and redaction software, offering products that speed workflows, increase efficiency and aid in regulation compliance. IGC solutions are deployed across almost every industry, with millions of installed seats worldwide. Learn more at www.infograph.com.

For more information,
please contact:

Informative Graphics Corp.
4835 E. Cactus Road, Suite 445
Scottsdale, AZ 85254
www.infograph.com
800.398.7005 (intl +1.602.971.6061)
sales@infograph.com