# Ensuring Security of High-Risk Information in EHRs

Save to myBoK

This practice brief has been retired. It is made available for historical purposes only.

---

Healthcare organizations are entrusted with the most private information of their patients and employees. They have a legal, moral, and ethical duty to protect all clinical and research information by ensuring that security and privacy safeguards are in place. A higher degree of control is necessary to prevent unauthorized access to especially sensitive information. This is particularly true within the context of the electronic health record (EHR).

This practice brief identifies categories of health information that are afforded special protections under law or may otherwise require a higher degree of security. It recommends system features and practices that will help secure sensitive information in EHRs and afford organizations satisfactory assurances that sufficient safeguards shield this information from misuse.

HIM professionals must be aware of high-risk groups and be able to assess whether electronic systems include features and functionality that may increase risk of inappropriate use and disclosure or offer additional layers of protections for sensitive information.

## Categories That May Warrant a Higher Degree of Security in an Electronic System

Highly sensitive health data involve certain conditions, tests, and records of vulnerable or high-profile patients and minors. Implementing security features for such categories can present challenges in EHRs because specific functionality may not be present in all systems or be fully evolved. The following categories provide examples.

### Patient Type and Identity

Consistent and reliable methods for authenticating patient identity and linking patients to their records warrant special security because they are essential to delivering quality care and improving patient safety.

There is great variability and incompatibility of patient identification systems in healthcare facilities, making it difficult to uniquely identify patients within one facility or between entities. A system of identifying patients between entities must exist for interoperability to occur. Currently, there are no record-to-record matching standards in the industry.

Safeguarding patient information is critical to preventing identity theft, medical identity theft, fraud, and abuse, and may be addressed through improved physical and logical access control systems and constant vigilance. Organizations require strict policies and procedures governing the use of physical media and portable devices to prevent theft or loss.

Special circumstances may arise in which patient identification or access to individual patient records may require anonymity or special precautions, such as in the case of celebrity or high-profile individuals, workplace privacy, domestic violence, child or vulnerable adult abuse, litigation, organ donors, and prisoners. In such cases, EHRs should enable use of a “record hold,” de-identification mechanism, access restriction, or alias to afford greater protection for a specified period of time.

### Diagnosis or Condition

The law affords special protection to certain diagnoses or conditions. Electronic systems must be able to identify and manage these types of data appropriately.

Mental health records are generally protected at a higher level of confidentiality, as they may contain a patient’s innermost personal information. Many of the individuals receiving service for mental health issues are vulnerable, and their privacy must

be protected to ensure they have the same considerations as others in the community and that they do not fall prey to identity theft or fraud.

HIV/AIDS and sexually transmitted diseases are another category with special privacy concerns. Public health reporting of these conditions is required, and the secure transmission of the information is a special consideration when working with electronic data.

When releasing HIV/AIDS records for other purposes, it is necessary to identify testing and treatment for these conditions through the use of flags or warning messages. An electronic system should facilitate exclusion or segregation of HIV test results to protect against release without appropriate consent from the patient. Ideally a system would also flag treatment of HIV/AIDS or a sexually transmitted disease when producing copies of records.

Substance abuse and chemical dependency records require special consideration beyond what has been identified for mental health and HIV/AIDS records. EHR systems must provide mechanisms that enable facilities to manage the extra layer of protection for this information required under 42 CFR, Part 2, particularly for release of information purposes. Release of these records requires special authorization clearly indicating the patient's consent. When released, these records must include a written statement prohibiting redisclosure by the recipient.

Patients have a right to revoke an authorization to release records in writing or verbally, and institutions must have mechanisms to track and comply with this requirement. Records in this category are not released in response to a subpoena unless accompanied by the patient's signed consent or valid court order.

In a multispecialty or acute care environment, management and security of these records can be challenging. Organizations must have the ability to segregate any records related to treatment of substance abuse and chemical dependency, as treatment of these patients can encompass multiple medical specialties and document types. EHR systems require continued development of functionality to manage security, add levels of security, block access to specific notes or lab results, track versioning, and mask sensitive entries for release of information.

## Privacy, Confidentiality, and Security

The HIPAA privacy and security rule requirements, as well as accrediting standards, complement each other. Individuals have the right to expect their health information will be kept confidential.

**Confidentiality** , for the purpose of this article, is the practice of permitting only certain authorized individuals to access information with the understanding that they will disclose it only to other authorized individuals as permitted by law. For example, substance abuse information may not be released without specific consent.

**Privacy** , for the purpose of this article, is an individual's right to control his or her protected health information.

**Security** is the protections or safeguards (administrative, technical, or physical) put in place to secure protected health information.

### Procedure and Testing

The controversy surrounding procedures, surgeries, and tests such as abortion, family planning, genetic testing, and cosmetic surgery makes the related clinical documentation a high-risk category. Abortion, family planning, and genetic testing are controversial due to personal and religious beliefs and insurance qualifications. Individuals, particularly public figures, are often scrutinized and harassed by the media for details regarding cosmetic surgery. HIM professionals should focus on increasing the security of this category in order to protect patient privacy and livelihood.

Electronic systems should enable the core security features of role-based access, passwords, and audit trails. It is also recommended that aliases or alternative account numbers be assigned to individuals undergoing special procedures or tests such as the ones listed here. The EHR must be able to connect the alias or alternative account number back to the patient's

legal name and account number in a secure fashion to ensure the individual has a complete medical record and to enable accurate billing while still protecting the privacy of the patient.

There are serious privacy issues related to genetic testing. Individuals are faced with a fear of employment discrimination or loss of health and life insurance based on apparent or perceived genetic abnormality. Currently, the fear of discrimination and misuse of genetic information prevents people from obtaining genetic testing. The refusal to use effective genetic tests hurts individuals, researchers, and physicians. Lack of testing denies individuals important medical information they could otherwise use to proactively manage their health.

The Genetic Information Nondiscrimination Act of 2008, signed into law in May 2008, prohibits discrimination on the basis of genetic information with respect to health insurance and employment. Additionally, 41 states already have enacted legislation related to genetic discrimination in health insurance, and 31 states have adopted laws regarding genetic discrimination in the workplace, according to the National Human Genome Research Institute.

The Council for Responsible Genetics notes that "in all cases, state and federal laws have primarily addressed the unlawful use of genetic data, sidestepping the question of whether employers and insurance companies should have access to genetic information in the first place."[1]

**Consent and Custody**

Issues of consent and custody may require the unique handling of health information if the patient is unable to consent to disclosures either permanently or temporarily due to health or legal status. Such patients include wards of the state, incapacitated or incompetent individuals, inmates or detainees, minors, minors in a custody conflict, and parties involved in adoptions. Records of the deceased are also included in this category.

Parents, guardians, or a designated individual who represents the interest of the patients that fall within this category are required by law to verify their right to access health information.

Inmates or detainees are unique in that they may lose rights to obtain their physical medical record under HIPAA. They are not permitted to have copies while they are incarcerated because of the possibility of danger to another inmate or staff member. If the facility deems this potential danger could occur, it must note the reason for withholding the record. Inmates have the ability to view and communicate their health status with their healthcare provider. After release from incarceration, the detainees regain the ability to receive copies of their health information.

Unemancipated minors require security of their protected health information. EHRs must have the functionality to adequately secure records for minors involved in child custody conflicts or adoptions. Recommended practices for protected access to health information of minors include:

- Identifying the necessary process. For example, the Indian Health Service guideline for release of information to insurance or law firms requires the person acting in loco parentis (collectively, "parent") to obtain the information and then disclose to a third party. Legal representatives should be consulted regarding guardianship, powers of attorney, and other related issues.
- Identifying the individual that has authority to access records.
- Implementing alerts or flags to identify patients in this category.
- Creating high security lockout access for these files with a VIP access code.

In most situations, minors must give consent prior to release of their substance abuse records.

**Research**

Data generated, collected, and reported in support of clinical trials by a clinical investigator at an investigative site are source data. They may be found in progress notes, patient diaries, orders, ECGs, x-rays, lab results, and other ancillary test results maintained by the healthcare facility as part of the patient's medical record.

Analysis of the data by the clinical investigator and study sponsor may lead to decisions about specific treatments (e.g., a drug's efficacy and safety). These data, when captured and stored electronically, are subject to FDA rules, specifically 21 CFR Part 11, which outlines security and electronic signature requirements for research records and research source documentation.

In addition to security practices recommended for EHRs in general (such as audit trails and role-based access), organizations should employ technical security features that identify, protect, and authenticate research records. These features include alerts to identify patients who are research subjects and clinical trial participants and unique document types for research notes and research consents.

Organizations should evaluate electronic signatures against the 21 CFR Part 11 standards and turn on available features such as unique ID and password entry at the time of each signing. Signature manifestations should include the printed name of the signer, date, time of signature execution, and meaning of the signature (such as approval or authorship).

## System Considerations for High-Risk Data

Organizations should seek EHR products that offer security features consistent with their needs. EHRs must have the ability to limit access and provide screening controls to only those staff working directly with the patient or those with administrative responsibilities (such as risk management, legal, and HIM). Screening controls should include the ability to redact sensitive information that should not be disclosed.

User activity must be tied to a unique user identification to reliably maintain an audit trail of navigation, documentation, and other activities. Audit trails are essential in tracking user activities such as document viewing, manual printing, addendums, retracted or restored documents, and follow-up requests. Document creation should be recorded, per user, with appropriate date and time stamps for when the document was saved, posted, validated, or otherwise electronically signed.

The organization's security efforts will benefit from a system's ability to map a record to a scanned copy of a release, power of attorney, or other legal document specifying the privileges of a personal or authorized representative. Organizations would also benefit from functionality that could require a user to enter justification for any manual printing as well as prevent unauthorized screen printing and unauthorized download to portable storage devices.

In the instance of a sentinel event or other pending legal process, the EHR should have the capability to move the record into a "restricted unit," which immediately locks down access and restricts it to personnel directly involved in the review, such as legal and risk management. Such functionality protects the record from being viewed by staff members curious about the incident details. The record can be "opened" to a particular staff member for a brief period of time if additional documentation needs to be entered, but the access should be limited.

Security features provide HIM professionals with the ability to track for security issues, such as inappropriate access and printing. Flags and alerts could provide a mapping of where else in the EHR specific data are located.

## Recommendations for HIM Professionals

HIM professionals, entrusted with the protection of data, must ensure that a given EHR system includes functionality that will enable the organization to meet its regulatory and operational requirements.

When it comes to protecting high-risk information, HIM professionals should identify the location of that information in the organization and verify state-specific guidelines related to the categories. They should identify functions in the electronic systems that create risk and limit or restrict their use with the sensitive record class. Likewise, they should identify security features that offer higher degrees of protection and implement their use to protect sensitive information. As the emphasis on the privacy and security protection of information continues to increase, in both public and professional sectors, vendors are enhancing the security features in their systems to accommodate the requirements needed for sensitive information.

When selecting an electronic system, organizations must evaluate the system independently and systematically and not rely solely on the vendor's interpretation of system functionality. If the system of choice requires implementation of additional security measures, the organization must determine if it will be able to do so without risking the security of, or access to, the

data. Approaching system selection from the perspective of the regulatory and operational impact will no doubt prove invaluable in its future use to both the organization and the individuals whose information it contains.

HIM professionals should partner with their IT counterparts and build a relationship of trust and teamwork, as both areas of expertise must join forces toward achieving the common goal of improving patient care through technology.

## Security Features Considerations

Handling highly sensitive information within an EHR requires distinct system features. Lack of these features can restrict the system's use with certain categories of high-risk data. Features that enable appropriate degrees of protection include:

- Role-based security that restricts access to predefined categories of patients, encounters, and documents based on the access a user needs to perform his or her job
- VIP status indicators that restrict especially identified patients and encounters to those individuals with permission for VIP encounters and patients
- Ability to assign an alias to a patient or encounter to mask patient identity
- Ability to restrict patients from physicians who are not the "physician of record" (e.g., attending, admitting, surgeon, and consulting)
- Ability to block access to a specific progress note or lab result
- Ability to track versioning or mask sensitive entries for release of information

Considerations around specific functions or situations include the following:

### Accessing Information from Locations outside the Organization's Control

Information accessed from outside the organization can pose risk. It is easy for an unidentified user to access the network if the remote connection is not secure. Laptops containing sensitive information that are removed from the organization must be protected in case of loss or theft.

- Is remote access into the network secure?
- Are laptops and other portable devices properly tracked? Are they encrypted and protected with security measures (e.g., passwords)?

### Transmission

Autofaxing, messaging, and e-mailing protected health information can create risk. For example, autofaxing may fail to confirm the intended recipient or that the transaction was completed. Messaging and e-mail bring similar risks but also must take into account the threat of hackers intercepting messages in transit.

- Are all transmissions encrypted?
- Are all transmissions tracked, and is an audit trail available?
- Can transmissions be blocked?

### IT Support

- What level of access do technical staff—both internal staff and vendor—need to support the system?
- Does system support require access to the application database where patient data are stored?
- Can all sensitive information be blocked from support staff's view and access?
- Can troubleshooting be achieved through the use of test data rather than live records?

- What means are used for remote support?
- For systems hosted by vendors, what audit trails are in place to monitor vendor staff activity? Does the vendor provide access to these logs?
- Are audit trails of routine maintenance available?

**Release of Information**

- Are features available to block printing and downloading of sensitive information?
- Can different levels of access be given to control the above?
- Are audit trails in place for these actions?

**Break-the-Glass Situations**

"Breaking the glass" refers to an authorized user's ability to override access restrictions in emergency situations while still providing for appropriate audit trail and disclosure log requirements.

- Who has the ability to enact this?
- How is it controlled?
- Is it auditable?
- Can access for sensitive information be excluded?

**Staff Training**

System functions alone do not ensure privacy and security. Organizations must have policies and procedures in place, and they must communicate and enforce them.

- Do employees receive appropriate and ongoing education on privacy and security policies?
- Does the organization maintain policies on data security?

## Note

1. Council for Responsible Genetics. "Genetic Testing, Discrimination, and Privacy." Available online at www.gene-watch.org/programs/privacy.html.

## References

Alfano, Sandra L. "Research Documentation and Data Security." Presentation. April 10, 2007. Available online at www.info.med.yale.edu/hic/docs/ResearchDoc-DataSecurity.ppt.

Amadeus International. "21 CFR Part 11 Best Practices." Available online at www.amadeussolutions.com/english/practices/bp_21cfr_part11.htm.

HIPAA, Public Law 104-191, 45 CFR §160.103 and 154.504.

HIPAA 45 CFR §164.510(b).

Indian Health Service, US Department of Health and Human Services. "Policy and Procedure for Protected Health Information of Un-emancipated Minors." Available online at www.ihs.gov/adminmngrresources/hipaa/training/pdf/pandp/UnemanicipatedMinorsPP31JAN03.pdf.

National Human Genome Institute. "Genetic Information Nondiscrimination Act: 2007–2008." Available online at www.genome.gov/24519851.

School of Government, the University of North Carolina at Chapel Hill. Available online at www.sog.unc.edu.

Substance Abuse and Mental Health Services Administration, US Department of Health and Human Services. "The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs." June 2004. Available online at www.hipaa.samhsa.gov/download2/SAMHSAHIPAAComparisonClearedPDFVersion.pdf.

US Food and Drug Administration. "Guidance for Industry: Computerized Systems Used in Clinical Trials." Available online at www.fda.gov/ora/compliance_ref/bimo/ffinalcct.htm

## Prepared By

AHIMA e-HIM Work Group on Security of Personal Health Information

Linda Barbera, MS
Teresa Costa, RHIT, CMT
Valerie Engel, RHIT
Regina Everett, MPA, RHIA
Jill Flanigan, RHIT
Cathy A. Flite, MEd, RHIA
Sheri Hutchins, MA, RHIA, CCS
Melissa Jarriel, RHIA, CTR, CHP
Elaine King, MHS, RHIA, CHP
Catherine Klug, MSN, RN
Johnna Morrell, RHIA
Gertrude Racette, RHIT, CHP
Marsha Steele, MEd, RHIA

## Acknowledgments

Angela K. Dinh, MHA, RHIA
Lou Ann Wiedemann, MS, RHIA, CPEHR

*This work was supported in part by FORE.*

---

The information contained in this practice brief reflects the consensus opinion of the the professionals who developed it. It has not been validated through scientific research.

---

**Article citation**:
AHIMA e-HIM Work Group on Security of Personal Health Information. "Ensuring Security of High-Risk Information in EHRs" *Journal of AHIMA* 79, no.9 (September 2008): 67-71.

---