

Overview of State Immunization Registries and Patient Confidentiality

Most states in the U.S. have an immunization information system (IIS), also known as an immunization registry, that collects immunization data for individuals in each state or municipality (some large cities host their own IIS). Though registries serve many purposes, two primary goals of an IIS are to maintain an active record of a patient's immunization history so that patients can receive appropriate vaccinations throughout their lifetime regardless of the site of administration, and for population-based surveillance of vaccination coverage to help control vaccine-preventable diseases. Each state has laws that govern reporting to an IIS, such as who must report, what must be reported, and whether individuals may opt-out of sharing their information with the registry. All states with registries collect data on child vaccinations (though the cut-off age varies by state) and most states now record adult immunizations as well.

At a minimum, states generally require that reported information include the patient's name (first, middle and last); date of birth; gender; address, including zip code; mother's maiden name; mother's or other responsible party's name (first, middle and last, including maiden name); and vaccine administration date, type, lot number and manufacturer. Although providers may enter this data manually into their state's IIS, many providers are now relying on the transfer of this information through a patient's electronic health record.

Requirements for inclusion of patient data in an IIS vary by state. For inclusion of child data, most states rely on the implied consent of a parent or guardian, with the ability to opt-out upon request. However, a few states mandate inclusion in the registry with no right to opt-out.¹ Mandatory inclusion in a state's registry may be limited to early childhood immunizations or particular vaccines.

Both state law and HIPAA govern provider sharing of a patient's vaccination information with a state IIS. Under HIPAA's public health exception, covered entities—including healthcare providers and health plans—may share a patient's private health information for public health purposes without the patient's consent. Such health information would include the patient's immunization records. HIPAA also requires providers to release a patient's health information to a public health authority upon request in the case of a public health emergency, which may be applicable to sharing of immunization data in the case of certain disease outbreaks. A growing number of states mandate that healthcare providers share patient immunization information with the state IIS (unless a patient opts-out), with providers subject to fines and other penalties for failure to report.

State laws require that patient information provided to an IIS be kept confidential. However, many states permit specified entities, such as schools, daycare centers, and camps, to access a child's immunization record

¹ Martin, D., Lowery, N., and Brand, B. et al. Immunization Information Systems: A Decade of Progress in Law and Policy, *Journal of Public Health Management and Practice*, 2013 00(00), 1-8.

through the registry to verify a child's immunization status. State laws govern the re-disclosure of this data, usually requiring that patient information retrieved from the IIS remain confidential and not subject to further disclosure without patient consent.

For more information on use of patient data for public health purposes, see

<http://www.healthinfo.org/article/big-data-and-public-health-navigating-privacy-laws-maximize-potential>.

For more information about HIPAA and exceptions to patient consent for public health purposes, see

<http://www.healthinfo.org/article/myth-buster-healthcare-providers-violate-hipaa-if-they-share-patient-information-public-he-0>.

Follow us on Twitter at [@HealthInfoLaw](https://twitter.com/HealthInfoLaw).