Statutory Summary: Falsification of Electronic Records and International Trafficking of Government Research Data

This document is a neutral legal analysis for informational purposes only and does not constitute legal advice.

Contents

1 Compact Statutory Summary Table

Compact Overview of Key Statutes

Reference	Code Summary	One Act Defined As:	Penalty & Charge Classification
18 U.S.C. §1035	False statements in health-care matters.	Each fabricated or materially false medical record or statement related to diagnosis, treatment, or health-care services.	Up to 5 years per count. Federal felony.
18 U.S.C. §1512	Witness tampering by intimidation, threats, or misleading conduct.	Use of falsified medical records or data to corruptly influence, discredit, or silence a witness or records custodian.	Up to 20 years depending on subsection. Federal felony.
18 U.S.C. §1519	Falsification of records in federal investigations.	Creating or altering medical records to impede or influence a matter within federal jurisdiction.	Up to 20 years. Federal felony.
18 U.S.C. §1028A	Aggravated identity theft.	Using another person's identifiers (patient, clinician, or witness) in committing specified felonies involving medical and research records.	Mandatory 2-year consecutive term. Federal felony with mandatory minimum.
18 U.S.C. §875(d)	Interstate extortionate threats to injure reputation.	Threatening release of falsified medical records or data to coerce or retaliate.	Up to 2 years. Federal felony.
18 U.S.C. §2261A	Interstate stalking/harassment.	Using falsified medical data across state lines to cause substantial emotional distress or intimidation.	Up to 5 years; up to 10 years if serious harm or weapons involved. Federal felony.
18 U.S.C. §1030 (CFAA)	Computer fraud and abuse.	Each intentional unauthorized access to obtain medical or research data used in falsified records.	Typically 5–10 years per count where aggravating factors are present. Federal felony.
18 U.S.C. §641	Theft or conversion of government records or research data (DARPA, NIH).	Each unauthorized obtaining, copying, or transmission of government-funded research data or files.	Up to 10 years if value $\geq$ \$1,000; otherwise up to 1 year. Federal felony (or misdemeanor under \$1,000).
18 U.S.C. §371	Conspiracy to commit any federal offense.	Agreement plus any overt act to falsify medical records, hack systems, or traffic government data.	Up to 5 years (or the maximum of the underlying misdemeanor). Federal felony in most applications.

Reference	Code Summary	One Act Defined As:	Penalty & Charge Classification
State Medical Record Falsification / Identity Misuse (NV, CA, TX, FL)	State offenses criminalizing fabrication of medical records and misuse of identity.	Each falsified medical entry, impersonation of a clinician, or misuse of another's identifiers in medical documentation.	Generally 1–5 years; enhanced for financial gain or repeated conduct. Usually a state felony; some misdemeanor variants.
State Defamation / Criminal Libel	False statements causing reputational harm, including false medical claims.	Publishing knowingly false medical information to damage reputation.	Civil damages; in some states, up to 1 year confinement for criminal libel. Civil cause of action; in some jurisdictions, state misdemeanor.
International Trafficking of Data & Falsified Records (Selected Jurisdictions)	Movement of stolen or falsified data across borders.	Each transfer of DARPA/NIH data or falsified medical records via physical media or electronic transmission, including exchanges for gifts or cash.	Typically charged as U.S. federal felonies (export, conspiracy, theft) plus foreign offenses (cybercrime, document fraud, identity misuse).

2 Expanded Statutory Summary Table (Longtable Format)

Expanded Statutory Summary: Falsification of Medical Records and Related Conduct

Reference	Code Summary	One Act Defined As:	Penalty & Charge Classification
18 U.S.C. §1035 (False Statements in Health-Care Matters)	Criminalizes knowingly and willfully making materially false statements or documents in connection with health-care matters.	Each fabricated medical record, altered entry, or materially false statement relating to diagnosis, treatment, billing, or health-care documentation, including falsified records used to undermine a witness's testimony.	Penalty: Up to 5 years per count. Classification: Federal felony.
18 U.S.C. §1512 (Witness Tampering)	Prohibits intimidation, threats, corrupt persuasion, or misleading conduct toward another person, with intent to influence, delay, or prevent testimony or cooperation with authorities.	Each act of using falsified medical records or data, or threatening to publish them, in order to corruptly influence, discredit, or silence a witness or records custodian in a federal proceeding or investigation.	Penalty: Up to 20 years depending on the subsection and circumstances (e.g., official proceedings, threats, physical force). Classification: Federal felony.
18 U.S.C. §1519 (Falsification of Records in Federal Investigations)	Prohibits knowingly altering, destroying, concealing, or falsifying documents to impede or influence the investigation or administration of any matter within federal jurisdiction.	Each creation, alteration, or concealment of medical records, DARPA/NIH data, or related documentation, where done with intent to interfere with testimony, an investigation, or regulatory review.	Penalty: Up to 20 years imprisonment. Classification: Federal felony.
18 U.S.C. §1028A (Aggravated Identity Theft)	Imposes a mandatory consecutive term for using another person's identifying information during certain predicate felonies (including fraud, computer crimes, and health-care offenses).	Each use of patient, clinician, or witness identifiers (names, account numbers, signatures, credentials) to fabricate or authenticate falsified medical records or to transmit stolen government data during qualifying felonies.	Penalty: Mandatory 2-year term per count, served consecutively to any underlying sentence. Classification: Federal felony with mandatory minimum.
18 U.S.C. §875(d) (Interstate Extortionate Threats)	Prohibits using interstate communications to threaten injury to a person's reputation, property, or person with intent to extort anything of value.	Each interstate communication threatening to release falsified medical records or altered DARPA/NIH data to coerce a victim to recant, remain silent, or provide money, favors, or other value.	Penalty: Up to 2 years for subsection (d); other subsections involving violent threats can reach up to 5 years. Classification: Federal felony.

Reference	Code Summary	One Act Defined As:	Penalty & Charge Classification
18 U.S.C. §2261A (Interstate Stalking / Harassment)	Criminalizes using interstate or foreign communications to harass, intimidate, or cause substantial emotional distress.	Each instance of interstate or international dissemination of falsified medical information, fabricated diagnoses, or altered health data intended to cause substantial emotional distress or to intimidate a witness, especially when transmitted across state or national borders.	Penalty: Up to 5 years; up to 10 years where bodily injury, dangerous weapons, or pattern of conduct elevates the offense. Classification: Federal felony.
18 U.S.C. §1030 (Computer Fraud and Abuse Act)	Prohibits intentional unauthorized access to protected computers (including health systems and research servers) to obtain information or further fraud.	Each intentional unauthorized access—or access exceeding authorization—used to obtain non-public medical records, DARPA/NIH research files, or other data later falsified or used to fabricate evidence.	Penalty: Typically 5–10 years for offenses involving furtherance of fraud, damage, or value thresholds; enhanced for repeat offenders or national security implications. Classification: Federal felony.
18 U.S.C. §2701 (Stored Communications Act)	Prohibits unauthorized access to stored electronic communications or data.	Each unauthorized access to cloud-stored medical records, email systems, or document repositories containing the original records or DARPA/NIH files used in the falsification scheme.	Penalty: Up to 1 year for basic violations; up to 5 years for commercial advantage, malicious harm, or repeated conduct. Classification: Typically a federal misdemeanor; becomes a federal felony under aggravating circumstances.
18 U.S.C. §641 (Theft or Conversion of Government Records and Research Data)	Prohibits theft, conversion, unauthorized copying, or dissemination of U.S. government property, including government-funded research data (DARPA, NIH).	Each unauthorized obtaining, copying, retention, or transmission of DARPA- or NIH-associated data or software (including approximate valuation near $10,000,000), whether conveyed physically or electronically, and regardless of classification status.	Penalty: Up to 10 years where property value is $1,000 or more; up to 1 year when value is under $1,000. Classification: Federal felony if value $\geq$ $1,000; otherwise federal misdemeanor.
18 U.S.C. §371 (Conspiracy)	Criminalizes agreement by two or more persons to commit any federal offense and the commission of any overt act in furtherance.	Each coordinated plan to hack systems, obtain DARPA/NIH data, fabricate or alter medical records, or disseminate falsified materials to undermine testimony or obstruct federal processes.	Penalty: Up to 5 years, or the maximum penalty of the underlying misdemeanor if the target offense is not a felony. Classification: Federal felony in most contexts.

Reference	**Code Summary**	**One Act Defined As:**	**Penalty & Charge Classification**
State Defamation / Criminal Libel (Varies by State)	Prohibits intentional publication of knowingly false statements causing reputational harm.	Each act of publishing knowingly false medical claims or diagnostic information about a victim intended to defame or damage reputation.	Penalty: Civil damages (actual and punitive); in some states, criminal libel carries up to 1 year of incarceration. Classification: Primarily civil cause of action; in some jurisdictions, a state misdemeanor.
State Identity Misuse / Medical Record Falsification (e.g., NV, CA, TX, FL)	Criminalizes intentional misuse of identity or fabrication/alteration of medical records at the state level.	Each falsified medical entry, impersonation of a patient or clinician, or use of another's identifying information in health records or related documentation. Applies to conduct in Nevada, California, Texas, and Florida.	Penalty: Typically 1–5 years incarceration; enhanced penalties when conduct is repeated, financially motivated, or part of a broader fraud scheme. Classification: Generally a state felony; some states maintain misdemeanor variants depending on the value or harm.
International Trafficking of U.S. Medical or Research Data (Argentina, Australia, Belgium, Britain, Canada, Curaçao, Ireland, Jamaica, Scotland, Trinidad & Tobago)	Movement of stolen or falsified data (including DARPA/NIH files and fabricated medical records) across international borders, whether by physical device or electronic transmission.	Each act of transporting devices carrying DARPA/NIH data, transmitting falsified medical records or government research to counterparts abroad, or exchanging such material for gifts or cash while traveling through or operating in Argentina, Australia, Belgium, Britain, Canada, Curaçao, Ireland, Jamaica, Scotland, Trinidad, or Tobago.	Relevant U.S. charges may include: – 18 U.S.C. §554 (smuggling/export violations), – 18 U.S.C. §1832 (theft of trade secrets / economic espionage where applicable), – 18 U.S.C. §641 (government records), – 18 U.S.C. §371 (conspiracy), – 18 U.S.C. §1030 (CFAA). Classification: U.S. federal felonies; parallel foreign felonies for cybercrime, document fraud, identity misuse, and data trafficking.

3 Jurisdiction-by-Jurisdiction Appendix

This appendix summarises how international trafficking or transmission of DARPA/NIH research data and falsified medical records may be treated in the listed jurisdictions. It does not provide an exhaustive survey of each country's statutes but outlines typical categories of exposure.

Jurisdiction	**Illustrative Treatment of Trafficking / Data Misuse**	**Cooperation / Interaction with U.S. Proceedings**
Argentina	Data protection, computer crime, and document fraud statutes may criminalize possession, transfer, or use of stolen or falsified medical and research data.	Subject to mutual legal assistance frameworks and extradition arrangements with the United States; U.S. charges (e.g., conspiracy, computer fraud, theft of government property) may proceed parallel to local enforcement.
Australia	Comprehensive cybercrime and fraud statutes address unauthorized access, data theft, and use of false documents; handling stolen research data may be prosecuted as computer offenses or fraud.	Formal extradition treaty and cooperation in cybercrime investigations; dual criminality principles typically satisfied by overlapping offenses.
Belgium	Penal provisions on forgery, fraud, and unauthorized access to information systems can cover falsified medical records and illicit research data.	Cooperates with U.S. through EU and bilateral agreements for mutual legal assistance and extradition; local prosecution may run alongside U.S. federal proceedings.
Britain (United Kingdom)	Computer Misuse Acts and fraud/forgery laws criminalize hacking, data theft, and use of false documents, including medical and research records.	Extradition treaty and robust law-enforcement cooperation with the U.S.; U.K. authorities may assist in evidence gathering and, where appropriate, extradition.
Canada	Criminal Code provisions address unauthorized use of computers, fraud, identity theft, and possession of stolen data; falsified health records may trigger additional liability under health and privacy regimes.	Extradition treaty and strong MLAT cooperation with the U.S.; investigations often coordinated where conduct spans both jurisdictions.
Curaçao (Kingdom of the Netherlands)	Local laws, aligned with Dutch criminal law, may criminalize unauthorized data access, possession of stolen digital information, and document falsification.	Cooperation typically occurs through the Kingdom of the Netherlands and associated treaties; U.S. authorities may seek assistance in tracing data flows or devices.
Ireland	Statutes on computer misuse, fraud, and document forgery apply to trafficking of stolen or falsified medical and research records within or through Ireland.	Mutual legal assistance and extradition mechanisms exist between Ireland and the U.S.; cybercrime and data-tracing cooperation are common.
Jamaica	Anti-fraud and cybercrime frameworks may apply to handling or transmitting stolen health and research data or falsified medical documentation.	Extradition and cooperation arrangements with the U.S. facilitate evidence sharing and, in appropriate cases, transfer of suspects.

Jurisdiction	**Illustrative Treatment of Trafficking / Data Misuse**	**Cooperation / Interaction with U.S. Proceedings**
Scotland (United Kingdom)	Scottish criminal law (including fraud, forgery, and computer misuse offenses) covers unauthorized access, data theft, and falsified documents involving medical and research records.	As part of the U.K., Scotland participates in U.S.–U.K. extradition and MLAT processes; investigative support may be provided for U.S. proceedings.
Trinidad and Tobago	Cybercrime and fraud statutes may criminalize the trafficking or use of stolen or falsified medical and research materials, especially where used for financial gain or reputational harm.	Extradition and cooperation frameworks with the U.S. allow for mutual assistance in transnational cyber and fraud investigations.

End of statutory summary. This document is for analytical and educational use only and is not legal advice.