RESOLUTION NO. 09-21-02

THE BOARD OF COUNTY COMMISSIONERS OF THE COUNTY OF DOLORES STATE OF COLORADO

A RESOLUTION ADOPTING A POLICY REGARDING THE HANDLING OF PERSONAL IDENTIFYING INFORMATION (PII) INCLUDING PROTECTION, DESTRUCTION AND SECURITY BREACH REPORTING

At a regular meeting of the Board of County Commissioners of Dolores County (BOCC) held in Dove Creek, Colorado on the 20th day of September 2021, with the following persons present:

Commissioners present: Floyd Cook (Chair), Julie Kibel, Steve Garchar

Commissioners absent:

County Attorney: Dennis R. Golbricht

Deputy Clerk to the BOCC: Jody Gardner

IT WAS RESOLVED:

WHEREAS, C.R.S. §§24-73-101, 102, and 103 ("Security Breaches and Personal Information Statutes"), require, among other things, that when a governmental entity maintains paper or electronic documents that contain "personal identifying information," as that term is defined in C.R.S. § 24-73-101(4)(b), the governmental entity develop a written policy for the destruction and proper disposal of such documents; and

WHEREAS, the Security Breaches and Personal Information Statutes also require governmental entities that maintain, own, or license personal identifying information to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the governmental entity; and

WHEREAS, the Security Breaches and Personal Information Statutes also require governmental entities that maintain, own, or license computerized data that includes "personal information" about a Colorado resident to conduct an investigation into, and under certain circumstances, provide notice of, a "security breach," as such terms are defined in C.R.S. § 24-73-103(1)(g) and (h), respectively; and

WHEREAS, Dolores County maintains paper or electronic documents that contain personal identifying information, and maintains, or may maintain in the future, computerized data that includes personal information about Colorado residents; and

WHEREAS, in accordance with the Security Breaches and Personal Information Statutes, the BOCC desires to establish policies and procedures regarding the destruction or disposal of paper or electronic documents that contain personal information and personal identifying information, reasonable security procedures and practices regarding personal information and personal identifying information, and investigation and notification requirements related to potential security breaches of personal information.

NOW, THEREFORE, BE IT RESOLVED THAT THE FOLLOWING POLICY IS HEREBY ADOPTED EFFECTIVE IMMEDIATELY:

Section 1. Definitions

"Biometric Data" means unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account.

"Departments" means, collectively, all departments under the supervision and control of the Dolores County Commissioners and all County elected officials' offices with the consent of the elected official.

"Determination that a Security Breach Occurred" means the point in time at which there is sufficient evidence to conclude that a security breach has taken place.

"Dolores County" means Dolores County, Colorado, acting by and through the Dolores County Board of County Commissioners.

"Encrypted" means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

"Medical Information" means any information about a consumer's medical or mental health treatment or diagnosis by a health care professional.

"Notice" means:

- written notice to the postal address listed in the records of the governmental entity;
- telephonic notice;
- electronic notice, if a primary means of communication by the governmental entity with a Colorado resident is by electronic means or the notice provided is consistent with the provisions regarding electronic records and signatures set forth in the federal "electronic signatures in global and national commerce act," 15 U.S.C. sec. 7001 *et seq*.; or
- substitute notice, if the governmental entity required to provide notice demonstrates that the cost of providing notice will exceed two hundred fifty thousand dollars, the affected class of persons to be notified exceeds two hundred fifty thousand Colorado residents, or

the governmental entity does not have sufficient contact information to provide notice substitute notice consists of all of the following:

- e-mail notice if the governmental entity has e-mail addresses for the members of the affected class of Colorado residents;
- conspicuous posting of the notice on the website page of the governmental entity if the governmental entity maintains one; and
- notification to major statewide media.

"Personal identifying information" means, a social security number; a personal identification number; a password; a passcode; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, as defined in C.R.S § 6-1-716(1)(a); an employer, student, or military identification number; or a financial transaction device, as defined in section C.R.S. §18-5-701(3).

"Personal Information" means (A) a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: social security number; driver's license number or identification card number; student, military, or passport identification number; medical information; health insurance identification number; or biometric data, as defined in this section; (B) a Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; or (C) a Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

> **"Personal Information"** does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

"Security Breach" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a governmental entity good faith acquisition of personal information by an employee or agent of a governmental entity for the purposes of the governmental entity is not a security breach if the personal information is not used for a purpose unrelated to the lawful government purpose or is not subject to further unauthorized disclosure.

The definitions of the Security Breaches and Personal Information Statutes are further hereby incorporated into this Policy to the extent not set forth above.

Section 2. DISPOSAL OF PERSONAL IDENTIFYING INFORMATION

It shall be the policy for all Departments that, unless otherwise required by state or federal law or regulation, when any paper or electronic documents containing personal identifying information are no longer needed by the Departments, the Departments shall destroy or arrange for the destruction of such paper and electronic documents within the Departments' custody or control by shredding, erasing, or otherwise modifying the personal identifying information in the paper or

electronic documents to make the personal identifying information unreadable or indecipherable through any means. The Departments shall implement inter-departmental procedures and policies which address the specific nature of their offices to ensure compliance with this Policy and the Security Breaches and Personal Information Statutes.

Section 3. PROTECTION OF PERSONAL IDENTIFYING INFORMATION

All Departments shall protect personal identifying information from unauthorized access, use, modification, disclosure, or destruction. The Departments, with assistance from the Information Technologies Department, shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information given the nature of Dolores County and its size as a governmental entity.

The Departments shall require that in all contracts with third parties, which either do, or could result in, the exchange of personal identifying information, contractual terms to ensure third parties are subject to, and abiding by, the terms of the Security Breaches and Personal Information Statutes and this Policy.

Section 4. NOTIFICATION OF SECURITY BREACH

The Departments shall immediately notify the County Administrator and the IT Director when it becomes aware that a Security Breach may have occurred. The Departments shall conduct a good faith prompt investigation to determine the likelihood that personal information has been or will be misused. Dolores County shall give Notice, as provided below, to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur.

Notice shall be made in the most expedient time possible and without unreasonable delay, but not later than thirty (30) days after the date of determination that a Security Breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

In the event Dolores County is required to provide Notice, as defined in Section 1, the following information shall be provided to all affected Colorado residents:

- the date, estimated date, or estimated date range of the security breach;
- a description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach;
- information that the resident can use to contact the governmental entity to inquire about the security breach;
- the toll-free numbers, addresses, and websites for consumer reporting agencies;
- the toll-free number, address, and website for the federal trade commission; and
- a statement that the resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

If an investigation by Dolores County determines that personal information has been misused or is reasonably likely to be misused, then Dolores County shall, in addition to the notice otherwise required by above, and in the most expedient time possible and without unreasonable delay, but not later than thirty (30) days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system:

- Direct the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same username or e-mail address and password or security question or answer.

- For log-in credentials of an e-mail account furnished by Dolores County, Dolores County shall not comply with this section by providing the security breach notification to that e-mail address, but may instead comply with this section by providing notice through other methods, as defined in Section 3, or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an internet protocol address or online location from which Dolores County knows the resident customarily accesses the account.

The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or was reasonably believed to have been acquired.

Departments are prohibited from charging the cost of providing such notice to individuals.

If the Departments use a third-party service provider to maintain computerized data that includes personal information, then the Departments shall require that the third-party service provider shall give notice to and cooperate with Dolores County in the event of a security breach that compromises such computerized data, including notifying Dolores County of any security breach in the most expedient time and without unreasonable delay following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with Dolores County information relevant to the security breach; except that such cooperation does not require the disclosure of confidential business information or trade secrets.

Section 5. REPORTING OF SECURITY BREACH

If Dolores County must notify Colorado residents of a data breach pursuant to this Policy, then Dolores County shall provide notice of any security breach to the Colorado Attorney General in the most expedient time possible and without unreasonable delay, but not later than thirty (30) days after the date of determination that a security breach occurred, if the security breach is reasonably believed to have affected five hundred Colorado residents or more, unless the

investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur.

The breach of encrypted or otherwise secured personal information must be disclosed in accordance with this section if the confidential process, encryption key, or other means to decipher the secured information was also acquired or was reasonably believed to have been acquired in the security breach.

If Dolores County is required to notify more than one thousand (1,000) Colorado residents of a security breach pursuant to this Policy, Dolores County shall also notify, in the most expedient time possible and without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal "Fair Credit Reporting Act", 15 U.S.C. sec. 1681a (p), of the anticipated date of the notification to the residents and the approximate number of residents who are to be notified. Nothing in this Policy requires Dolores County to provide to the consumer reporting agency the names or other personal information of security breach notice recipients. This Section 6 does not apply to a person who is subject to Title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 *et seq*.

A waiver of these notification rights or responsibilities is void as against public policy.

*****

Unanimously adopted by the BOCC this 20th day of September 2021.

_____
Floyd Cook (Chair)

_____
Julie Kibel

_____
Steve Garchar

DEPUTY CLERK TO THE BOARD

_____
Jody Gardner